



Table of Contents

1.	Categories of data (subscriber information, traffic data, content data).....	2
1.1.	Definitions under national legislation	2
2.	Procedures for Preservation Requests of stored computer data	3
2.1	Expedited Preservation of stored computer data (Art. 29)	3
2.2	Expedited Disclosure for Stored Traffic Data (Art. 30)	3
3.	Procedures for Mutual Legal Assistance	5
3.1	Requests for Stored Computer Data: Subscriber, Traffic, Content Data (Art. 31)	5
3.2	Requests for Real Time Collection of Traffic Data (Art. 33)	16
3.3	Requests for Interception of Content Data (Art. 34).....	16

This information sheet has been prepared by the Cybercrime Programme Office (C-PROC) of the Council of Europe in view of facilitating international cooperation. It does not necessarily reflect official positions of the State covered or of the Council of Europe.

1. Categories of Data (subscriber information, traffic data, content data)

1.1. Definitions under national legislation

Subscriber Information <reference to the law if applicable>	<definition if applicable>
Traffic Data Law No. 5651, Art 2	" IP addresses of the parties, beginning and ending time of the offered service, type of the benefited service, amount of transferred data and -if available- subscriber's information"
Content Data <reference to the law if applicable>	<definition if applicable>

<General comment as to whether Domestic law distinguishes subscriber information from that of traffic and / or content data, whether the same or different rules of procedure apply to obtaining of all types of data>

2. Procedures for preservation requests of stored computer data

2.1 Expedited preservation of stored computer data (Art. 29)

General remarks

Procedures in place

1. Confirmation of receipt (30 minutes)
2. Legal review as to the national and international requirements (1-2 hours)
3. Sending back for additional clarifications, proceeding with the request or refusing to comply
4. In case it goes forward - verification with the prosecutor/supervisor (if necessary)
5. Sending the request for execution to provider/person and waiting for response
6. Follow up in cases of urgency or where specific time for response was requested and there is no feedback from provider

Article 29 of Convention on Cyber Crimes regulates the Quick Declaration of Stored Computer Data; and Article 30 of the said convention regulates the Quick Declaration of Preserved Traffic Data. The Traffic Data was defined as follows in the Article 2 of Law No. 5651: " IP addresses of the parties, beginning and ending time of the offered service, type of the benefited service, amount of transferred data and -if available- subscriber's information"

According to Article 5/3 of Law No. 5651, hosting service providers are obliged to save the traffic data of the hosting services that they provide, for a period of time not less than one year and not more than two years, which shall be designated by the regulations, and are also obliged to ensure the accuracy, integrity and confidentiality of these data.

According to Article 6/1-b of Law No. 5651, access providers are obliged to save the traffic data of the services that they provide, for a period of time not less than six months and not more than two years, which shall be designated by the regulations, and are also obliged to ensure the accuracy, integrity and confidentiality of these data.

In Turkey, the central authority in international legal assistance is the General Directorate of International Law and Foreign Relations, Ministry of Justice. In addition to this, requests within the scope of Articles 29 and 30 of the Convention, are not coming in the form of legal assistance requests.

2.2 Expedited disclosure for stored traffic data (Art. 30)

General remarks

Procedures in place

1. Confirmation of receipt (30 minutes)
2. Legal review as to the national and international requirements (1-2 hours)
3. Sending back for additional clarifications, proceeding with the request or refusing to comply
4. In case it goes forward - verification with the prosecutor/supervisor (if necessary)

5. Sending the request for execution to provider/person and waiting for response
6. Follow up in cases of urgency or where specific time for response was requested and there is no feedback from provider

Article 29 of Convention on Cyber Crimes regulates the Quick Declaration of Stored Computer Data; and Article 30 of the said convention regulates the Quick Declaration of Preserved Traffic Data. The Traffic Data was defined as follows in the Article 2 of Law No. 5651: " IP addresses of the parties, beginning and ending time of the offered service, type of the benefited service, amount of transferred data and -if available- subscriber's information"

According to Article 5/3 of Law No. 5651, hosting service providers are obliged to save the traffic data of the hosting services that they provide, for a period of time not less than one year and not more than two years, which shall be designated by the regulations, and are also obliged to ensure the accuracy, integrity and confidentiality of these data.

According to Article 6/1-b of Law No. 5651, access providers are obliged to save the traffic data of the services that they provide, for a period of time not less than six months and not more than two years, which shall be designated by the regulations, and are also obliged to ensure the accuracy, integrity and confidentiality of these data.

In Turkey, the central authority in international legal assistance is the Ministry of Justice, Directorate General of Foreign Relations and European Union Affairs. In addition to this, requests within the scope of Articles 29 and 30 of the Convention, are not coming in the form of legal assistance requests

3. Procedures for mutual legal assistance

3.1 Requests for stored computer data: subscriber, traffic, content data (Art. 31)

»» Go to [Subscriber information](#) | [Traffic Data](#) | [Content Data](#)

► Requests for subscriber information

General remarks

Turkey ratified the European Convention on Mutual Assistance in Criminal Matters, its additional protocols and the European Convention on Extradition.

Turkey cooperates with other countries on the basis of the generic legal framework, the [Law no. 6706](#) on International Legal Cooperation in Criminal Matters.

According to Article 5 of the Law no. 6706 while executing the request for judicial cooperation, the provisions of the Criminal Procedure Code dated 04/12/2004 and numbered 5271 shall be applied in the cases which are not provided for by this Law and the other Laws.

It includes preservation and expedited disclosure of every crime within international cooperation (Article 7), access to computer data within international cooperation (Article 7 and 8), comprising search, seizure and disclosure of data stored in the computer system located in Turkey, when the search and seizure would be admissible in a similar national case and interception of communications within international cooperation (sub para. (a) of the first paragraph for Article 8).

Article 8 allows foreign authorities, without prior request from the Turkish authorities, to access data stored in a computer system located in Turkey, where publicly available or access through a computer system located in its territory, the data stored in Turkey, through legal and voluntary consent of the person legally authorised to disclose them

Competent Authorities

Ministry of Justice, Directorate General of Foreign Relations and European Union Affairs is the designated central authority for mutual legal assistance in criminal matters.

The legal competence to commence and direct criminal investigations belongs to the Prosecution Service, with the technical support from the police. It is also the competence of the Prosecution Service to send and to receive international cooperation requests.

In compliance with Article 35 of the Budapest Convention, a 24/7 point of contact was established, since 2011, and it is based in the National Cybercrime Department (TNP). The same structure is used for the G8 network purposes and also for the INTERPOL Network.

[Back to the Table of Contents](#)

The National Cybercrime Department has specific competence in undertaking urgent measures related to expedited preservation of traffic data. It could conduct urgent searches and seizure of data on the basis of a judicial authorisation under Article 134 of Code No. 5271 on "search of computers, computer programs and transcripts, copying and provisional seizure. Besides, local police forces play a significant role in combating cybercrime. They carry out operations and investigate cybercrime at the local level."

Relevant contact points

The request can be made directly to Interpol Ankara NCB, if it is thought that it may cause delay, the following address can be used as well.

Turkish National Police
Department of Cybercrime
İncekMah. Boztepe Sk. No: 125
06830 İncekGölbaşı-ANKARA
cyber.ncp@egm.gov.tr

Prior consultations

It is not required. It is optional.

24/7 contact point exists.

Accepted legal basis / mechanisms for MLA requests

Conventions of European Council are the primary reference regarding legal assistance. As for the other countries, if there is a bilateral convention between the states, then these conventions are referred to; otherwise "principle of reciprocity" is to be implemented. The following are the key conventions in this field;

- European Convention on Mutual Assistance in Criminal Matters (ETS No. 30)
- Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters
- Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters (ETS No. 182)
- Convention on Cybercrime (ETS- No. 185)
- Other Conventions regarding legal assistance.

In the national level;

- Law No. 6706 regarding International Legal Cooperation in Criminal Matters
- Circulars of Ministry of Justice

Content of the request

In the legal assistance request; the requesting authority, reason of the request and the request, an explanation of the legal incident regarding the request, personal information of the subject of the request should be mentioned and legal grounds text should be attached. If there is a "Bilateral Convention" between the states, this convention must be referred to in the section of legal grounds. Relevant court decrees and statutory basis must be also annexed to this letter of request.

Applicable legal requirements

The term "data" was defined as "all kinds of value which can be processed by the computer", while the term "traffic data" was defined as "IP addresses of the parties, beginning and ending time of the offered service, type of the benefited service, amount of transferred data and -if available- subscriber's information" in the Article 2 of Law No. 5651. In this regard, legal requirements for obtaining subscriber data related to criminal investigation and prosecution has been regulated by the Article 135 and 140 of Law No. 5271, Turkish Code of Criminal Procedure. (Article 135 and 140 of Turkish Code of Criminal Procedure will be written here)

Detection, interception and recording of communication
Article 135. –

“(1) If during a crime investigation, there are strong indications of suspicion based on concrete evidences that a crime has been committed and there are no other means of collecting evidence, with the decision of the judge or where a delay is detrimental with the decision of the public prosecutor, the communications of the suspect or the accused may be intercept and recorded their signal datas may be evaluated by means of telecommunications. In such case, the public prosecutor shall immediately submit his decision to the judge for approval and the judge shall decide on this matter within twenty four hours, at the latest. Upon expiry of this period or if the judge denies approval, such measure shall be lifted by the public prosecutor immediately.

2) A Report or document showing the user if being known and the person with communication mean or the communication line to be given a rulling of measure in accordance with the article shall be added.

(3) The suspect's communication with persons who are entitled to refrain from acting as a witness shall not be recorded. If such a situation is understood after the recording, the recorded material shall be destroyed immediately.

(4) In the decision to be taken in accordance with paragraph one, the type of the crime attributed, the identity of the person for whom such a measure is to be implemented, the type of communication means, telephone number or the code that allows for the detection of the communication line, the type of measure, its scope and duration shall be stated. Such a measure can be ruled for two months, at the most; however this period can be extended for just a month not more than 3 months in total.

(5) In order to apprehend the suspect or the accused, the place of the mobile phone used by the suspect or the accused can be detected by a judge's decision and where a delay may be detrimental by the public prosecutor's decision. In the decision taken for this purpose, the number of the mobile phone and the duration of the detection process shall be indicated. Detection process can be performed for a period of three months, at the most; however this period can be extended for just a month.

(6) Detection of the accused and the suspect's the communications by means of telecommunication shall be made on the grounds of a decision of judge or where a delay is detrimental with a decision of public prosecutor in the investigation process and in case of procecution period with the decision of the court in prosecution process. In the decision the type of the crime attributed, the identity of the person for whom such a measure is to be implemented, the type of communication means, telephone number or the code that allows for the detection of the communication line and the duration of measure shall be stated. The public prosecutor shall immediately submit his decision to the judge for approval and the judge shall decide on this matter within twenty four hours, at the latest. Upon expiry of this period or if the judge denies approval, such measure shall be lifted by the public prosecutor immediately.

(7) The decision taken and the actions made according to the provisions of this article shall be kept confidential during the period in which such measure is implemented.

(8) The provisions of this article shall only apply with regard to the below listed offences:

a) In the Turkish Penal Code;

1. Migrants smuggling and trafficking in human beings (Articles 79, 80) and trading of organs and tissues(Art. 91),
2. Deliberate killing (Articles 81, 82, 83),
3. Torture (Articles 94, 95),
4. Sexual assault (excluding the first paragraph, Article 102),
5. Sexual abuse of children (Article 103),

6. Aggravated theft (Art. 142), robbery(Art. 148,149) and aggravated fraud(Art. 158),
 7. Manufacturing and trafficking of drugs and stimulant (Article 188),
 8. Counterfeiting of money (Article 197),
 9. Establishing an organisation with the aim of committing crimes (excluding paragraphs three, Article 220),
 10. Prostitution (Art.227)
 11. Bid rigging (Article 235),
 12. Usury (Art. 241),
 13. Bribery (Article 252),
 14. Laundering the proceeds obtained through criminal activity (Article 282),
 15. Disrupting the unity and integrity of the state (Art. 302),
 16. Offences against the constitutional order and its functioning (Art. 309, 311, 312, 313, 314, 315, 316)
 17. Espionage and crimes against state secrets (Article 328, 329, 330, 331, 333, 334, 335, 336, 337)
- b) Arms smuggling as defined in the Law on Fire Arms and Knives and Other Tools (Article 12)
- c) The crimes which necessitate imprisonment as a punishment in the Anti-Smuggling Law.
- d) The crimes defined in Articles 68 and 74 of the Law on the Preservation of Cultural and Natural Heritage.
- (9) Apart from the principles and procedures laid down in this Article, no one can monitor or record the communication of another person through telecommunications."

Surveillance with technical means

"Article 140 –

- (1) If there are strong indications of suspicion *based on concrete evidences* that crimes listed below have been committed, and if there is no other available means of obtaining evidence, the activities of the suspect or the accused, conducted in fields open to the public and his working places, may be subject to surveillance by technical means, including voice and image recording;
- a) Crimes regulated in the Turkish Criminal Code;
1. Migrants smuggling and trafficking in human beings (Articles 79, 80) and trading of organs and tissues(Art. 91),
 2. Deliberate killing (Articles 81, 82, 83),
 3. Aggravated theft (Art. 142), robbery(Art. 148,149) and aggravated fraud(Art. 158),
 4. Manufacturing and trafficking of drugs and stimulant (Article 188),
 5. Counterfeiting of money (Article 197),
 6. Establishing an organisation with the aim of committing crimes (excluding paragraphs three, Article 220),
 7. Prostitution (Art.227)
 8. Bid rigging (Article 235),
 9. Usury (Art. 241),
 10. Bribery (Article 252),
 11. Laundering the proceeds obtained through criminal activity (Article 282),
 12. Disrupting the unity and integrity of the state (Art. 302),
 13. Offences against the constitutional order and its functioning (Art. 309, 311, 312, 313, 314, 315, 316)
 14. Espionage and crimes against state secrets (Article 328, 329, 330, 331, 333, 334, 335, 336, 337)
- b) Arms smuggling as defined in the Law on Fire Arms and Knives and Other Tools (Article 12)
- c) The crimes which necessitate imprisonment as a punishment in the Anti-Smuggling Law.
- d) The crimes defined in Articles 68 and 74 of the Law on the Preservation of Cultural and Natural Heritage."

Confidentiality requirements

When information request from ISPs, it is preferred to ask via BTK which is governmental regulating authorities. If needed we also contact directly to ISPs. There is no specific legislation about requesting or receiving information from ISPs. The information requests are made in frame of general provisions.

Urgent requests

If we receive a request that provides us that there is an exigent emergency involving the danger of death or serious physical injury to a person, we do prioritize the request to prevent that harm. The requests we receive should contain enough evidence that we can share with the relevant authorities when asked.

Translation

Information can be obtained from here, regarding the requests coming to 7/24 Contact Center. A Turkish translation must be definitely provided in requests drawn up in the form of legal assistance requests. Besides, within the scope of European Convention on Mutual Assistance in Criminal Matters, it may be sufficient to transmit the requests between party states, in English. In general, language of the relevant state and a Turkish translation are accepted to be sufficient.

Limitations

A court decree is sought in this regard. Subject of the request must only be used limited to the request.

► Requests for Traffic Data

General remarks

Competent Authorities

Within the scope of Article 135 of Turkish Code of Criminal Procedure, as long as there is a competent judge's decision, subscribers' data can be demanded through a legal assistance request which can be sent to Ministry of Justice, Directorate General of Foreign Relations and European Union Affairs.

Judicial authorities like Public Prosecutor's Offices and Courts in Turkey, can demand subscribers' data through sending their requests to the Ministry of Justice, Directorate General of Foreign Relations and European Union Affairs. According to Turkish Law, prior confirmation or decision of a judge (even in **where a delay is detrimental with the decision of the public prosecutor** is for approval), is mandatory, regarding the issue.

Relevant contact points

The request can be made directly to Interpol Ankara NCB, if it is thought that it may cause delay, the following address can be used as well.

Turkish National Police
Department of Cybercrime
İncekMah. Boztepe Sk. No: 125

06830 İncekGölbaşı-ANKARA
cyber.ncp@egm.gov.tr

Prior consultations

It is not required. It is optional.

24/7 contact point exists.

Accepted legal basis / mechanisms for MLA requests

Conventions of European Council are the primary reference regarding legal assistance. As for the other countries, if there is a bilateral convention between the states, then these conventions are referred to; otherwise "principle of reciprocity" is to be implemented. The following are the key conventions in this field;

- European Convention on Mutual Assistance in Criminal Matters (ETS No. 30)
- Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters
- Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters (ETS No. 182)
- Convention on Cybercrime (ETS- No. 185)
- Other Conventions regarding legal assistance.

In the national level;

- Law No. 6706 regarding International Legal Cooperation in Criminal Matters
- Circulars of Ministry of Justice

Content of the request

In the legal assistance request; the requesting authority, reason of the request and the request, an explanation of the legal incident regarding the request, personal information of the subject of the request should be mentioned and legal grounds text should be attached. If there is a "Bilateral Convention" between the states, this convention must be referred to in the section of legal grounds. Relevant court decrees and statutory basis must be also annexed to this letter of request.

Applicable legal requirements

The term "data" was defined as " all kinds of value which can be processed by the computer", while the term "traffic data" was defined as "IP addresses of the parties, beginning and ending time of the offered service, type of the benefited service, amount of transferred data and -if available- subscriber's information" in the Article 2 of Law No. 5651. In this regard, legal requirements for obtaining subscriber data related to criminal investigation and prosecution has been regulated by the Article 135 and 140 of Law No. 5271, Turkish Code of Criminal Procedure. (Article 135 and 140 of Turkish Code of Criminal Procedure will be written here)

Detection, interception and recording of communication
Article 135. –

“(1) If during a crime investigation, there are strong indications of suspicion based on concrete evidences that a crime has been committed and there are no other means of collecting evidence, with the decision of the judge or where a delay is detrimental with the decision of the public prosecutor, the communications of the suspect or the accused may be intercept and recorded their signal datas

may be evaluated by means of telecommunications. In such case, the public prosecutor shall immediately submit his decision to the judge for approval and the judge shall decide on this matter within twenty four hours, at the latest. Upon expiry of this period or if the judge denies approval, such measure shall be lifted by the public prosecutor immediately.

2) A Report or document showing the user if being known and the person with communication mean or the communication line to be given a rulling of measure in accordance with the article shall be added.

(3) The suspect's communication with persons who are entitled to refrain from acting as a witness shall not be recorded. If such a situation is understood after the recording, the recorded material shall be destroyed immediately.

(4) In the decision to be taken in accordance with paragraph one, the type of the crime attributed, the identity of the person for whom such a measure is to be implemented, the type of communication means, telephone number or the code that allows for the detection of the communication line, the type of measure, its scope and duration shall be stated. Such a measure can be ruled for two months, at the most; however this period can be extended for just a month not more than 3 months in total.

(5) In order to apprehend the suspect or the accused, the place of the mobile phone used by the suspect or the accused can be detected by a judge's decision and where a delay may be detrimental by the public prosecutor's decision. In the decision taken for this purpose, the number of the mobile phone and the duration of the detection process shall be indicated. Detection process can be performed for a period of three months, at the most; however this period can be extended for just a month.

(6) Detection of the accused and the suspect's the communications by means of telecommunication shall be made on the grounds of a decision of judge or where a delay is detrimental with a decision of public prosecutor in the investigation process and in case of procecuton period with the decision of the court in prosecution process. In the decision the type of the crime attributed, the identity of the person for whom such a measure is to be implemented, the type of communication means, telephone number or the code that allows for the detection of the communication line and the duration of measure shall be stated. The public prosecutor shall immediately submit his decision to the judge for approval and the judge shall decide on this matter within twenty four hours, at the latest. Upon expiry of this period or if the judge denies approval, such measure shall be lifted by the public prosecutor immediately.

(7) The decision taken and the actions made according to the provisions of this article shall be kept confidential during the period in which such measure is implemented.

(8) The provisions of this article shall only apply with regard to the below listed offences:

a) In the Turkish Penal Code;

1. Migrants smuggling and trafficking in human beings (Articles 79, 80) and trading of organs and tissues(Art. 91),
2. Deliberate killing (Articles 81, 82, 83),
3. Torture (Articles 94, 95),
4. Sexual assault (excluding the first paragraph, Article 102),
5. Sexual abuse of children (Article 103),
6. Aggravated theft (Art. 142), robbery(Art. 148,149) and aggravated fraud(Art. 158),
7. Manufacturing and trafficking of drugs and stimulant (Article 188),
8. Counterfeiting of money (Article 197),
9. Establishing an organisation with the aim of committing crimes (excluding paragraphs three, Article 220),
10. Prostitution (Art.227)
11. Bid rigging (Article 235),
12. Usury (Art. 241),
13. Bribery (Article 252),
14. Laundering the proceeds obtained through criminal activity (Article 282),
15. Disrupting the unity and integrity of the state (Art. 302),
16. Offences against the constitutional order and its functioning (Art. 309, 311, 312, 313, 314, 315, 316)
17. Espionage and crimes against state secrets (Article 328, 329, 330, 331, 333, 334, 335, 336, 337)

b) Arms smuggling as defined in the Law on Fire Arms and Knives and Other Tools (Article 12)

c) The crimes which necessitate imprisonment as a punishment in the Anti-Smuggling Law.

d) The crimes defined in Articles 68 and 74 of the Law on the Preservation of Cultural and Natural Heritage.

(9) Apart from the principles and procedures laid down in this Article, no one can monitor or record the communication of another person through telecommunications."

Surveillance with technical means

"Article 140 –

(1) If there are strong indications of suspicion *based on concrete evidences* that crimes listed below have been committed, and if there is no other available means of obtaining evidence, the activities of the suspect or the accused, conducted in fields open to the public and his working places, may be subject to surveillance by technical means, including voice and image recording;

a) Crimes regulated in the Turkish Criminal Code;

1. Migrants smuggling and trafficking in human beings (Articles 79, 80) and trading of organs and tissues(Art. 91),

2. Deliberate killing (Articles 81, 82, 83),

3. Aggravated theft (Art. 142), robbery(Art. 148,149) and aggravated fraud(Art. 158),

4. Manufacturing and trafficking of drugs and stimulant (Article 188),

5. Counterfeiting of money (Article 197),

6. Establishing an organisation with the aim of committing crimes (excluding paragraphs three, Article 220),

7. Prostitution (Art.227)

8. Bid rigging (Article 235),

9. Usury (Art. 241),

10. Bribery (Article 252),

11. Laundering the proceeds obtained through criminal activity (Article 282),

12. Disrupting the unity and integrity of the state (Art. 302),

13. Offences against the constitutional order and its functioning (Art. 309, 311, 312, 313, 314, 315, 316)

14. Espionage and crimes against state secrets (Article 328, 329, 330, 331, 333, 334, 335, 336, 337)

b) Arms smuggling as defined in the Law on Fire Arms and Knives and Other Tools (Article 12)

c) The crimes which necessitate imprisonment as a punishment in the Anti-Smuggling Law.

d) The crimes defined in Articles 68 and 74 of the Law on the Preservation of Cultural and Natural Heritage."

Confidentiality requirements

When information request from ISPs, it is preferred to ask via BTK which is governmental regulating authorities. If needed we also contact directly to ISPs. There is no specific legislation about requesting or receiving information from ISPs. The information requests are made in frame of general provisions.

Urgent requests

If we receive a request that provides us that there is an exigent emergency involving the danger of death or serious physical injury to a person, we do prioritize the request to prevent that harm. The requests we receive should contain enough evidence that we can share with the relevant authorities when asked.

Translation

Information can be obtained from here, regarding the requests coming to 7/24 Contact Center. A Turkish translation must be definitely provided in requests drawn up in the form of legal assistance

requests. Besides, within the scope of European Convention on Mutual Assistance in Criminal Matters, it may be sufficient to transmit the requests between party states, in English. In general, language of the relevant state and a Turkish translation are accepted to be sufficient.

Limitations

A court decree is sought in this regard. Subject of the request must only be used limited to the request.

► Requests for Content Data

General remarks

Competent Authorities

Within the scope of Article 135 of Turkish Code of Criminal Procedure, as long as there is a competent judge's decision, subscribers' data can be demanded through a legal assistance request which can be sent to the Ministry of Justice, Directorate General of Foreign Relations and European Union Affairs.

Judicial authorities like Public Prosecutor's Offices and Courts in Turkey, can demand subscribers' data through sending their requests to the Ministry of Justice, Directorate General of Foreign Relations and European Union Affairs. According to Turkish Law, prior confirmation or decision of a judge (even in **where a delay is detrimental with the decision of the public prosecutor** is for approval), is mandatory, regarding the issue.

Relevant contact points

The request can be made directly to Interpol Ankara NCB, if it is thought that it may cause delay, the following address can be used as well.

Turkish National Police
Department of Cybercrime
İncekMah. Boztepe Sk. No: 125
06830 İncekGölbaşı-ANKARA
cyber.ncp@egm.gov.tr

Prior consultations

It is not required. It is optional.

24/7 contact point exists.

Accepted legal basis / mechanisms for MLA requests

Conventions of European Council are the primary reference regarding legal assistance. As for the other countries, if there is a bilateral convention between the states, then these conventions are referred to; otherwise "principle of reciprocity" is to be implemented. The following are the key conventions in this field;

- European Convention on Mutual Assistance in Criminal Matters (ETS No. 30)
- Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters
- Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters (ETS No. 182)
- Convention on Cybercrime (ETS- No. 185)
- Other Conventions regarding legal assistance.

In the national level;

- Law No. 6706 regarding International Legal Cooperation in Criminal Matters
- Circulars of Ministry of Justice

Content of the request

In the legal assistance request; the requesting authority, reason of the request and the request, an explanation of the legal incident regarding the request, personal information of the subject of the request should be mentioned and legal grounds text should be attached. If there is a "Bilateral Convention" between the states, this convention must be referred to in the section of legal grounds. Relevant court decrees and statutory basis must be also annexed to this letter of request.

Applicable legal requirements

The term "data" was defined as " all kinds of value which can be processed by the computer", while the term "traffic data" was defined as "IP addresses of the parties, beginning and ending time of the offered service, type of the benefited service, amount of transferred data and -if available- subscriber's information" in the Article 2 of Law No. 5651. In this regard, legal requirements for obtaining subscriber data related to criminal investigation and prosecution has been regulated by the Article 135 and 140 of Law No. 5271, Turkish Code of Criminal Procedure. (Article 135 and 140 of Turkish Code of Criminal Procedure will be written here)

Detection, interception and recording of communication
Article 135. –

“(1) If during a crime investigation, there are strong indications of suspicion based on concrete evidences that a crime has been committed and there are no other means of collecting evidence, with the decision of the judge or where a delay is detrimental with the decision of the public prosecutor, the communications of the suspect or the accused may be intercept and recorded their signal datas may be evaluated by means of telecommunications. In such case, the public prosecutor shall immediately submit his decision to the judge for approval and the judge shall decide on this matter within twenty four hours, at the latest. Upon expiry of this period or if the judge denies approval, such measure shall be lifted by the public prosecutor immediately.

2) A Report or document showing the user if being known and the person with communication mean or the communication line to be given a rulling of measure in accordance with the article shall be added.

(3) The suspect’s communication with persons who are entitled to refrain from acting as a witness shall not be recorded. If such a situation is understood after the recording, the recorded material shall be destroyed immediately.

(4) In the decision to be taken in accordance with paragraph one, the type of the crime attributed, the identity of the person for whom such a measure is to be implemented, the type of communication means, telephone number or the code that allows for the detection of the communication line, the type of measure, its scope and duration shall be stated. Such a measure can be ruled for two months, at the most; however this period can be extended for just a month not more than 3 months in total.

(5) In order to apprehend the suspect or the accused, the place of the mobile phone used by the suspect or the accused can be detected by a judge’s decision and where a delay may be detrimental

by the public prosecutor's decision. In the decision taken for this purpose, the number of the mobile phone and the duration of the detection process shall be indicated. Detection process can be performed for a period of three months, at the most; however this period can be extended for just a month.

(6) Detection of the accused and the suspect's the communications by means of telecommunication shall be made on the grounds of a decision of judge or where a delay is detrimental with a decision of public prosecutor in the investigation process and in case of prosecution period with the decision of the court in prosecution process. In the decision the type of the crime attributed, the identity of the person for whom such a measure is to be implemented, the type of communication means, telephone number or the code that allows for the detection of the communication line and the duration of measure shall be stated. The public prosecutor shall immediately submit his decision to the judge for approval and the judge shall decide on this matter within twenty four hours, at the latest. Upon expiry of this period or if the judge denies approval, such measure shall be lifted by the public prosecutor immediately.

(7) The decision taken and the actions made according to the provisions of this article shall be kept confidential during the period in which such measure is implemented.

(8) The provisions of this article shall only apply with regard to the below listed offences:

a) In the Turkish Penal Code;

1. Migrants smuggling and trafficking in human beings (Articles 79, 80) and trading of organs and tissues(Art. 91),
 2. Deliberate killing (Articles 81, 82, 83),
 3. Torture (Articles 94, 95),
 4. Sexual assault (excluding the first paragraph, Article 102),
 5. Sexual abuse of children (Article 103),
 6. Aggravated theft (Art. 142), robbery(Art. 148,149) and aggravated fraud(Art. 158),
 7. Manufacturing and trafficking of drugs and stimulant (Article 188),
 8. Counterfeiting of money (Article 197),
 9. Establishing an organisation with the aim of committing crimes (excluding paragraphs three, Article 220),
 10. Prostitution (Art.227)
 11. Bid rigging (Article 235),
 12. Usury (Art. 241),
 13. Bribery (Article 252),
 14. Laundering the proceeds obtained through criminal activity (Article 282),
 15. Disrupting the unity and integrity of the state (Art. 302),
 16. Offences against the constitutional order and its functioning (Art. 309, 311, 312, 313, 314, 315, 316)
 17. Espionage and crimes against state secrets (Article 328, 329, 330, 331, 333, 334, 335, 336, 337)
- b) Arms smuggling as defined in the Law on Fire Arms and Knives and Other Tools (Article 12)
- c) The crimes which necessitate imprisonment as a punishment in the Anti-Smuggling Law.
- d) The crimes defined in Articles 68 and 74 of the Law on the Preservation of Cultural and Natural Heritage.

(9) Apart from the principles and procedures laid down in this Article, no one can monitor or record the communication of another person through telecommunications."

Surveillance with technical means

"Article 140 –

(1) If there are strong indications of suspicion *based on concrete evidences* that crimes listed below have been committed, and if there is no other available means of obtaining evidence, the activities of the suspect or the accused, conducted in fields open to the public and his working places, may be subject to surveillance by technical means, including voice and image recording;

a) Crimes regulated in the Turkish Criminal Code;

1. Migrants smuggling and trafficking in human beings (Articles 79, 80) and trading of organs and tissues(Art. 91),
2. Deliberate killing (Articles 81, 82, 83),
3. Aggravated theft (Art. 142), robbery(Art. 148,149) and aggravated fraud(Art. 158),
4. Manufacturing and trafficking of drugs and stimulant (Article 188),

5. Counterfeiting of money (Article 197),
 6. Establishing an organisation with the aim of committing crimes (excluding paragraphs three, Article 220),
 7. Prostitution (Art.227)
 8. Bid rigging (Article 235),
 9. Usury (Art. 241),
 10. Bribery (Article 252),
 11. Laundering the proceeds obtained through criminal activity (Article 282),
 12. Disrupting the unity and integrity of the state (Art. 302),
 13. Offences against the constitutional order and its functioning (Art. 309, 311, 312, 313, 314, 315, 316)
 14. Espionage and crimes against state secrets (Article 328, 329, 330, 331, 333, 334, 335, 336, 337)
- b) Arms smuggling as defined in the Law on Fire Arms and Knives and Other Tools (Article 12)
- c) The crimes which necessitate imprisonment as a punishment in the Anti-Smuggling Law.
- d) The crimes defined in Articles 68 and 74 of the Law on the Preservation of Cultural and Natural Heritage.”

Confidentiality requirements

When information request from ISPs, it is preferred to ask via BTK which is governmental regulating authorities. If needed we also contact directly to ISPs. There is no specific legislation about requesting or receiving information from ISPs. The information requests are made in frame of general provisions.

Urgent requests

If we receive a request that provides us that there is an exigent emergency involving the danger of death or serious physical injury to a person, we do prioritize the request to prevent that harm. The requests we receive should contain enough evidence that we can share with the relevant authorities when asked.

Translation

Information can be obtained from here, regarding the requests coming to 7/24 Contact Center. A Turkish translation must be definitely provided in requests drawn up in the form of legal assistance requests. Besides, within the scope of European Convention on Mutual Assistance in Criminal Matters, it may be sufficient to transmit the requests between party states, in English. In general, language of the relevant state and a Turkish translation are accepted to be sufficient.

Limitations

A court decree is sought in this regard. Subject of the request must only be used limited to the request.

3.2 Requests for real time collection of traffic data (Art. 33)

General remarks

Mutual assistance shall be governed by the conditions and procedures provided for under domestic law no 6706 regarding International Legal Cooperation in Criminal Matters

Competent Authorities

The Central Authority is Ministry of Justice, International Law and Foreign Relations Department.

Web: www.uhdigm.adalet.gov.tr

Relevant contact points

Prior consultations

Accepted legal basis / mechanisms for MLA requests

Content of the request

Applicable legal requirements

Confidentiality requirements

Urgent requests

Translation

Limitations

3.3 Requests for interception of content data (Art. 34)

General remarks

Competent Authorities

Within the scope of Article 135 of Turkish Code of Criminal Procedure, as long as there is a competent judge's decision, subscribers' data can be demanded through a legal assistance request which can be sent to the Ministry of Justice, Directorate General of Foreign Relations and European Union Affairs.

Judicial authorities like Public Prosecutor's Offices and Courts in Turkey, can demand subscribers' data through sending their requests to the Ministry of Justice, Directorate General of Foreign Relations and European Union Affairs. According to Turkish Law, prior confirmation or decision of a judge (even in **where a delay is detrimental with the decision of the public prosecutor** is for approval), is mandatory, regarding the issue.

Relevant contact points

The request can be made directly to Interpol Ankara NCB, if it is thought that it may cause delay, the following address can be used as well.

Turkish National Police
Department of Cybercrime
İncekMah. Boztepe Sk. No: 125
06830 İncekGölbaşı-ANKARA
cyber.ncp@egm.gov.tr

Prior consultations

It is not required. It is optional.

24/7 contact point exists.

Accepted legal basis / mechanisms for MLA requests

Conventions of European Council are the primary reference regarding legal assistance. As for the other countries, if there is a bilateral convention between the states, then these conventions are referred to; otherwise "principle of reciprocity" is to be implemented. The following are the key conventions in this field;

- European Convention on Mutual Assistance in Criminal Matters (ETS No. 30)
- Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters
- Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters (ETS No. 182)
- Convention on Cybercrime (ETS- No. 185)
- Other Conventions regarding legal assistance.

In the national level;

- Law No. 6706 regarding International Legal Cooperation in Criminal Matters
- Circulars of Ministry of Justice

Content of the request

In the legal assistance request; the requesting authority, reason of the request and the request, an explanation of the legal incident regarding the request, personal information of the subject of the request should be mentioned and legal grounds text should be attached. If there is a "Bilateral Convention" between the states, this convention must be referred to in the section of legal grounds. Relevant court decrees and statutory basis must be also annexed to this letter of request.

Applicable legal requirements

The term "data" was defined as " all kinds of value which can be processed by the computer", while the term "traffic data" was defined as "IP addresses of the parties, beginning and ending time of the

offered service, type of the benefited service, amount of transferred data and -if available-subscriber's information" in the Article 2 of Law No. 5651. In this regard, legal requirements for obtaining subscriber data related to criminal investigation and prosecution has been regulated by the Article 135 and 140 of Law No. 5271, Turkish Code of Criminal Procedure. (Article 135 and 140 of Turkish Code of Criminal Procedure will be written here)

Detection, interception and recording of communication
Article 135. –

“(1) If during a crime investigation, there are strong indications of suspicion based on concrete evidences that a crime has been committed and there are no other means of collecting evidence, with the decision of the judge or where a delay is detrimental with the decision of the public prosecutor, the communications of the suspect or the accused may be intercept and recorded their signal datas may be evaluated by means of telecommunications. In such case, the public prosecutor shall immediately submit his decision to the judge for approval and the judge shall decide on this matter within twenty four hours, at the latest. Upon expiry of this period or if the judge denies approval, such measure shall be lifted by the public prosecutor immediately.

2) A Report or document showing the user if being known and the person with communication mean or the communication line to be given a rulling of measure in accordance with the article shall be added.

(3) The suspect’s communication with persons who are entitled to refrain from acting as a witness shall not be recorded. If such a situation is understood after the recording, the recorded material shall be destroyed immediately.

(4) In the decision to be taken in accordance with paragraph one, the type of the crime attributed, the identity of the person for whom such a measure is to be implemented, the type of communication means, telephone number or the code that allows for the detection of the communication line, the type of measure, its scope and duration shall be stated. Such a measure can be ruled for two months, at the most; however this period can be extended for just a month not more than 3 months in total.

(5) In order to apprehend the suspect or the accused, the place of the mobile phone used by the suspect or the accused can be detected by a judge’s decision and where a delay may be detrimental by the public prosecutor’s decision. In the decision taken for this purpose, the number of the mobile phone and the duration of the detection process shall be indicated. Detection process can be performed for a period of three months, at the most; however this period can be extended for just a month.

(6) Detection of the accused and the suspect’s the communications by means of telecommunication shall be made on the grounds of a decision of judge or where a delay is detrimental with a decision of public prosecutor in the investigation process and in case of procecution period with the decision of the court in prosecution process. In the decision the type of the crime attributed, the identity of the person for whom such a measure is to be implemented, the type of communication means, telephone number or the code that allows for the detection of the communication line and the duration of measure shall be stated. The public prosecutor shall immediately submit his decision to the judge for approval and the judge shall decide on this matter within twenty four hours, at the latest. Upon expiry of this period or if the judge denies approval, such measure shall be lifted by the public prosecutor immediately.

(7) The decision taken and the actions made according to the provisions of this article shall be kept confidential during the period in which such measure is implemented.

(8) The provisions of this article shall only apply with regard to the below listed offences:

a) In the Turkish Penal Code;

1. Migrants smuggling and trafficking in human beings (Articles 79, 80) and trading of organs and tissues(Art. 91),
2. Deliberate killing (Articles 81, 82, 83),
3. Torture (Articles 94, 95),
4. Sexual assault (excluding the first paragraph, Article 102),
5. Sexual abuse of children (Article 103),
6. Aggravated theft (Art. 142), robbery(Art. 148,149) and aggravated fraud(Art. 158),
7. Manufacturing and trafficking of drugs and stimulant (Article 188),
8. Counterfeiting of money (Article 197),
9. Establishing an organisation with the aim of committing crimes (excluding paragraphs three, Article 220),

10. Prostitution (Art.227)
 11. Bid rigging (Article 235),
 12. Usury (Art. 241),
 13. Bribery (Article 252),
 14. Laundering the proceeds obtained through criminal activity (Article 282),
 15. Disrupting the unity and integrity of the state (Art. 302),
 16. Offences against the constitutional order and its functioning (Art. 309, 311, 312, 313, 314, 315, 316)
 17. Espionage and crimes against state secrets (Article 328, 329, 330, 331, 333, 334, 335, 336, 337)
- b) Arms smuggling as defined in the Law on Fire Arms and Knives and Other Tools (Article 12)
- c) The crimes which necessitate imprisonment as a punishment in the Anti-Smuggling Law.
- d) The crimes defined in Articles 68 and 74 of the Law on the Preservation of Cultural and Natural Heritage.
- (9) Apart from the principles and procedures laid down in this Article, no one can monitor or record the communication of another person through telecommunications."

Surveillance with technical means

"Article 140 –

- (1) If there are strong indications of suspicion *based on concrete evidences* that crimes listed below have been committed, and if there is no other available means of obtaining evidence, the activities of the suspect or the accused, conducted in fields open to the public and his working places, may be subject to surveillance by technical means, including voice and image recording;
- a) Crimes regulated in the Turkish Criminal Code;
1. Migrants smuggling and trafficking in human beings (Articles 79, 80) and trading of organs and tissues (Art. 91),
 2. Deliberate killing (Articles 81, 82, 83),
 3. Aggravated theft (Art. 142), robbery (Art. 148, 149) and aggravated fraud (Art. 158),
 4. Manufacturing and trafficking of drugs and stimulant (Article 188),
 5. Counterfeiting of money (Article 197),
 6. Establishing an organisation with the aim of committing crimes (excluding paragraphs three, Article 220),
 7. Prostitution (Art.227)
 8. Bid rigging (Article 235),
 9. Usury (Art. 241),
 10. Bribery (Article 252),
 11. Laundering the proceeds obtained through criminal activity (Article 282),
 12. Disrupting the unity and integrity of the state (Art. 302),
 13. Offences against the constitutional order and its functioning (Art. 309, 311, 312, 313, 314, 315, 316)
 14. Espionage and crimes against state secrets (Article 328, 329, 330, 331, 333, 334, 335, 336, 337)
- b) Arms smuggling as defined in the Law on Fire Arms and Knives and Other Tools (Article 12)
- c) The crimes which necessitate imprisonment as a punishment in the Anti-Smuggling Law.
- d) The crimes defined in Articles 68 and 74 of the Law on the Preservation of Cultural and Natural Heritage."

Confidentiality requirements

When information request from ISPs, it is preferred to ask via BTK which is governmental regulating authorities. If needed we also contact directly to ISPs. There is no specific legislation about requesting or receiving information from ISPs. The information requests are made in frame of general provisions.

Urgent requests

If we receive a request that provides us that there is an exigent emergency involving the danger of death or serious physical injury to a person, we do prioritize the request to prevent that harm. The requests we receive should contain enough evidence that we can share with the relevant authorities when asked.

Translation

Information can be obtained from here, regarding the requests coming to 7/24 Contact Center. A Turkish translation must be definitely provided in requests drawn up in the form of legal assistance requests. Besides, within the scope of European Convention on Mutual Assistance in Criminal Matters, it may be sufficient to transmit the requests between party states, in English. In general, language of the relevant state and a Turkish translation are accepted to be sufficient.

Limitations

A court decree is sought in this regard. Subject of the request must only be used limited to the request