Germany

International cooperation

Specific step-by-step procedures and best practices

Version 12 August 2020

Table of Contents

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.

www.coe.int/cybercrime

Back to the Table of Contents

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

1.1. Definitions under national legislation

Subscriber Information Section 3 point 3 of the Telecommunications Act (TKG) and section 14 paragraph 1 of the Telecommunication Media Act (TMG)	Subscriber information in terms of individual-related data is defined in section 3 point 3 of the Telecommunications Act (TKG) and section 14 paragraph 1 of the Telecommunication Media Act (TMG) as data of a participant, which are necessary for the establishment, content, modification or termination of a contractual relationship for telecommunication services.
Traffic Data Section 3 point 30 of the Telecommunications Act (TKG)	Pursuant to point 30 of Section 3 of the Telecommunications Act (TKG), traffic data are data collected, processed or used in the provision of a telecommunications service.
Content Data <reference to the law if applicable>	There is no definition of content data under German law. Content Data means the actual content of an electronic communication or storage process.

German law distinguishes not only between subscriber information itself from traffic and content data but also whether it is a telecommunications service or a telemedia service. For this reason, different rules of procedure apply depending on the type of data concerned and the context in which the communication takes place. The German Telecommunication Media Act (TMG) applies to all telemedia services, which comprises electronic information and communication services, unless they are telecommunication services. Insofar the German Telecommunications Act (TKG) is applicable.

Back to the Table of Contents

2. Procedures for preservation requests of stored computer data

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

General remarks

It was not necessary to explicitly implement the provisions of chapter III into German national law, because the general legal basis on which German authorities can cooperate already allows for the full extent of international cooperation as foreseen in these provisions. Even where no international treaties exist, the Act on International Cooperation in Criminal Matters enables German authorities to perform measures foreseen in the German Code of Criminal Procedure (StPO) also in execution of a request for MLA. This involves the measures specifically mentioned in this chapter.

Furthermore, under the German law the provisions of chapter III apply directly as far as they are in force in relation to the requesting country. This ensures, that all specific features and conditions of these provisions are taken into account.

However, it has to be stated that the institute of a preservation order doesn´t exist in German procedural law. Therefore, Article 29 of the Budapest Convention (Expedited preservation of stored computer data) has to be read in conjunction with Article 16[1]. This is because Article 16 specifies the national conditions which the parties must create. In Germany, this immediate backup can only be carried out by confiscating the data. However, this was already known during the negotiations on the Budapest Convention. Therefore, paragraph 1 of Article 16 clarifies "*Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data […]*".

The explanatory report complements this provision by saying: *"The reference to "order or similarly obtain" is intended to allow the use of other legal methods of achieving preservation than merely by means of a judicial or administrative order or directive (e.g. from police or prosecutor)."*

Procedures in place

According to German criminal procedural law, computer data is secured by confiscating the data carriers on which the data is stored. Preservation orders or a "quick freeze" procedure do not exist. Hence, the immediate backup regarding criminal investigations can only be executed by confiscating the data according to section 94, 95 and 98 of the German Code of Criminal Procedure (StPO).

Section 94 StPO prescribes that a criminal offence is suspected and that an object - e.g. the data – that may be of importance as evidence for the investigation shall be taken into custody or shall be otherwise secured. If the data are in the custody of a person and are not surrendered voluntarily, the data carriers have to be seized.

[1] As to Articles 16 and 29 on expedited preservation: Assessment report - Implementation of the preservation provisions of the Budapest Convention on Cybercrime – Adopted by the T-CY at its 8th Plenary (5-6 December 2012); 6.8 Germany
https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e722e

Back to the Table of Contents

In accordance to section 98 StPO the seizure may be ordered only by a court and - only in exigent circumstances - by the public prosecution office and its investigators.

If it is to be expected that the accused will not surrender the data voluntarily or in cases of urgent requests, a court search warrant according to section102, 105 StPO will be applied in addition to the seizure order to ensure that law enforcement authorities can access the data. Only under exigent circumstances, a search may also be ordered by the public prosecution office and its investigators.

In this context, it should be noted that the seizure of data according to German procedural law is a non-hidden investigation measure, a deferment of the notification of the person concerned is not provided for by law and therefore inadmissible. An obligation of confidentiality on the part of the provider is not possible in the case of an open search or a request for surrender under section 94 and 95 StPO. In so far the confidentiality that is required by Article 16 paragraph 3 of the Budapest Convention cannot be maintained.

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

General remarks

It was not necessary to explicitly implement the provisions of chapter III into German national law, because the general legal basis on which German authorities can cooperate already allows for the full extent of international cooperation as foreseen in these provisions. Even where no international treaties exist, the Act on International Cooperation in Criminal Matters enables German authorities to perform measures foreseen in the German Code of Criminal Procedure also in execution of a request for MLA. This involves the measures specifically mentioned in this chapter.

Furthermore, under the German law the provisions of chapter III apply directly as far as they are in force in relation to the requesting country. This ensures, that all specific features and conditions of these provisions are taken into account.

Procedures in place

The preservation and expedited disclosure of traffic data pursuant to section 3 point 30 and section 96 and 113b of the Telecommunications Act (TKG) in criminal investigations is regulated in section 100g StPO.

Section 100g StPO provides that if certain facts give rise to the suspicion that a person has committed an offence of substantial significance in the individual case or, in cases where there is criminal liability for attempt, has attempted to commit such an offence or has prepared such an offence by committing another offence or committed an offence by means of telecommunications, the traffic data may be captured insofar as this is necessary to establish the facts and capturing the data stands in appropriate relation to the importance of the matter.

The capture may be ordered by a court upon the application of the public prosecution office.

Back to the Table of Contents

The order shall be given in writing and it must also clearly designate the data to be transferred and the period during which they are to be transferred. Besides the operative part of the order shall indicate particularly the name and address of the person against whom the measure is directed, where known, the alleged offence on the basis of which the measure is being ordered and the type of information to be obtained by carrying out the measure and its relevance for the proceedings.

Only under exigent circumstances -e.g. in situations where a loss of data would be feared if the court were to intervene - the public prosecution office may also make the order, which has to be confirmed by a court within three days.

The amount of traffic data to be retained depends on the nature of the offence for which the defendant is charged. The storage of traffic data within the meaning of section 113b TKG (data retention) can only be considered where a criminal offence listed in section 100g paragraph 2 StPO has been committed).

At present German administrative courts have suspended the obligation to storage the data in respect of a complaint of two telecommunications service providers until a final decision is made as to whether the regulations are in conformity with European law. A reference for a preliminary ruling is currently pending before the European Court of Justice.

Back to the Table of Contents

3. Procedures for mutual legal assistance

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

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

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

German judicial authorities are able to cooperate with any other state irrespective of the fact whether an international bi- or multilateral treaty exists.

German law distinguishes the different data categories and measures for interception and collection of data, however, for mutual legal assistance, the same rules of procedure apply generally[2].
Information therefore is presented in a consolidated manner for all types of data and measures, with differences marked where applicable.

Competent Authorities

Generally, the German Federal Ministry of Justice and Consumer Protection (Bundesministerium der Justiz und für Verbraucherschutz) is competent for receiving mutual legal assistance requests from foreign states and for granting assistance.

However, the Federal Ministry of Justice and Consumer Protection has transferred that competence to the Federal Office of Justice (Bundesamt für Justiz).

Furthermore, a large part of this competence has been transferred to the governments of the German federal states (Bundesländer) who delegated it further to the local public prosecutor's offices and courts.

Depending on the legal basis on which the incoming request is based, the request needs to be directed to the federal authorities or directly to a local public prosecutor's office or courts. As a general rule, the latter are responsible for requests from member states of the European Union, while requests from states outside of the European Union shall be directed to the Federal Office of Justice.

There is no central authority responsible for receiving all incoming requests.

[2] As to mutual legal assistance: T-CY assessment report: The mutual legal assistance provisions of the Budapest Convention on Cybercrime – Adopted by the T-CY at its 12th Plenary (2-3 December 2014) https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726c
As well as: T-CY assessment report on mutual legal assistance: Follow up given by parties and observers – Adopted by T-CY 18 (27-28 November 2017) https://rm.coe.int/t-cy-2017-2-mla-follow-up-rep/168076d55f

Back to the Table of Contents

Relevant contact points

In case that a request needs to be send directly to a local public prosecutor's office or court, the EJN contact points or Eurojust can help to locate the respective authority.

Furthermore, the EJN Atlas can be useful even if the issuing authority is not another EU member state and therefore does not submit its request on the basis of an EU mutual legal assistance instrument: https://www.ejn-crimjust.europa.eu/ejn/AtlasChooseCountry/EN.

In case that the issuing authority needs to send the request to a federal authority or does not know the territorial link to Germany (e.g. the seat of the provider which holds the requested data), requests can be directed to the Federal Office of Justice (Bundesamt für Justiz):

Bundesamt für Justiz
Adenauerallee 99 - 103
53113 Bonn
Germany

Phone number: +49 228 99410 40
Fax number: +49 228 99410 5591
E-mail address: poststelle@bfj.bund.de

Futhermore, in compliance with Article 35 of the Budapest Convention, a 24/7 point of contact is established as part of the Federal Criminal Police Office (Bundeskriminalamt) in Wiesbaden, together with the G8 contact point and the Interpol contact point.

CC14 - Central Agency Cybercrime
Federal Criminal Police Office (Bundeskriminalamt)
Thaerstr. 11
65193 Wiesbaden
Germany

Phone number: +49 611 55 13101
Fax number: +49 611 55 45140
E-mail addresses: cc14-coc@bka.bund.de (non-urgent requests);
cc-officeronduty@bka.bund.de (urgent requests only)

Please note that although requests can be technically transmitted via 24/7 or Interpol – especially in urgent cases – it is always a judicial authority which is responsible for granting mutual legal assistance.

Prior consultations

Prior consultations are recommended to determinate the prospects of success of a mutual legal assistance request. Please note that German data retention rules are quite restrictive and for this reason, relevant data may only be stored and therefore available for a short period of time. For more information in regard to the current legal situation see above (point

Back to the Table of Contents

2.2). Furthermore, the real time collection of traffic data and the interception of content data is only possible when certain set of prerequisites is fulfilled.

Accepted legal basis / mechanisms for MLA requests

- Convention of 29 November 2001 on Cybercrime (Budapest Convention)
- Directive 2014/41/EU regarding the European Investigation Order in criminal matters
- Convention of 29 May 2000 on Mutual Assistance in Criminal Matters between the Member States of the European Union
- European Convention on Mutual Assistance in Criminal Matters of 20 April 1959
- Other bi- or multilateral treaties
- Reciprocity

Content of the request

In a request, please kindly provide all the relevant facts of your case concerning the investigated crimes as well as the applicable national law. It is also necessary to specify as exactly as possible the requested data and measure for obtainment of the data. The request should make clear how the requested data is linked to the investigated crime and why the data is necessary for the further investigation. If applicable, please also indicate the reasons why you believe that the respective data is located in Germany or could be obtained via a German authority.

Please state if the requested measure would be legal when carried out in the territory of your state as the requesting state. If your national law requires a court order to collect the requested data, please enclose a copy of that order (if necessary).

Depending on the chosen instrument for requesting mutual legal assistance, there might be other requirements concerning the form or the content of the request.

Applicable legal requirements

When executing a mutual legal assistance request in German territory, the provisions of German national law concerning the requested measure apply.

For the obtainment, collection and interception of data, a court warrant – or in certain cases: a posterior judicial confirmation – is necessary. Only the mere request of subscriber data does not require an authorization by a court.
Furthermore, real time collection and interception of data is only possible in cases of serious crimes (listed in the respective provisions of the German Code of Criminal Procedure) and the measure needs to be proportionate.

Please note that German court warrants concerning the real time collection and interception of data are limited to a maximum duration of three months into the future. If after that point further collection or interception is necessary, the court order needs to be renewed, which requires a respective further mutual legal assistance request.

Back to the Table of Contents

Confidentiality requirements

Confidentiality is a general principle in Germany that binds all authorities and courts. Furthermore, special requests for confidentiality from the issuing authority will generally be respected.

However, please note that under German law, certain persons affected by undercover measures (such as telecommunications surveillance, covert remote search of information technology systems, acoustic surveillance of private premises and outside of private premises, traffic data capture and technical investigation measures in respect of mobile terminals) need to be notified of the conducted measures as soon as possible without endangering the purpose of the investigation or other (legal) interests. The notification has to be given within 12 months (or 6 months for covert remote searches of information technology systems and acoustic surveillances of private premises) after completion of the measure at the latest, however it can be further deferred if a court approves. The court decides upon the duration of any further deferrals. The court may approve the permanent dispensation with notification if there is a probability bordering on certainty that the requirements for notification will not be fulfilled, even in the future.

These rules also apply to an incoming mutual legal assistance request requesting one of the mentioned measures on German territory.

Urgent requests

In general, according to domestic law German authorities must execute mutual law assistance requests immediately, i.e. without undue delay. Depending on the applicable legal mutual assistance instrument, specific time limits for the execution of the request may apply.

If a request is urgent, please indicate so at transmittal. Please also state the reasons why the request is urgent. The request will be prioritised and executed as soon as possible. Principally, German authorities prioritise cases involving (pre-trial) detention.

Translation

Incoming requests and their supporting documents need to be transmitted with a translation into German language, if an applicable treaty provision does not state otherwise.
In very urgent cases, an English version might be accepted, provided that a German translation will follow as soon as possible.

Limitations

Under German law, the rule of specialty applies to incoming mutual legal assistance requests. Therefore, the requesting state is only allowed to use the information provided

Back to the Table of Contents

from the German authorities for the purposes originally indicated in the request. Further use of the information is only possible with prior consent of the German authorities. In certain cases, the German authorities might formulate that condition or request a respective confirmation by the requesting state before transmitting the requested information. Furthermore, depending on the level of sensitivity of the data, the requesting state may need to confirm beforehand that it will delete the data if no longer needed for the national proceedings.

Back to the Table of Contents