formobile@netlaw.bg
Linkedin – Formobile-
Twitter – @Formobile2019
www.formobile-project.eu

IMPORTANT TO READ BEFORE ANSWERING THE QUESTIONNAIRE:

The FORMOBILE project is aimed at creating better mobile forensic tools to help combat crime more efficiently, enlarging the capacities of both first responders, common forensic laboratories and highly specialised laboratories and experts by providing them with better tools to acquire, decode, and analyse data coming from mobile devices. The majority of these tools will be integrated in the existing suite of MSAB software (XRY). Please refer to the FORMOBILE website for more information and especially to the work package breakdown of WPs 4-6: https://formobile-project.eu/project#.mod-wp-steps. It is essential to have this background to be able to accurately answer this questionnaire.

One of the aspects of the FORMOBILE project is to make sure that these tools are able to be used in the EU for the collection, decoding and analysis of information from mobile phones in a way that makes the obtained evidence admissible in court ("from crime scene to courtroom").

Hence, the questions that make up this questionnaire in essence aim to understand how mobile forensic tools aimed at retrieving, decoding and further analyzing information from a mobile device (e.g. a smartphone), are allowed in your jurisdiction under the applicable criminal law. We are especially interested in:

- whether technical measures may be used (and to what extent) to bypass security;
- to what extent the data on the mobile device may be read, searched, used and copied etc.;
- what the formal conditions are for accessing data on a mobile device;
- who must order such actions and in what level of detail the mandate must describe the authorized actions;
- in what scenarios this is permissible (only in certain scenarios, only if the phone belongs to the accused?), as well as the potential differences between scenarios;
- existing limits on the access to or further analyzing and use of the data on a mobile device.

formobile@netlaw.bg
Linkedin – Formobile-
Twitter – @Formobile2019
www.formobile-project.eu

In addition, we want to know under what conditions information on the Cloud can be accessed and if this is possible by technical means. We are also interested in any human rights' impacts, existing guidelines and issues in practice, existing case law and any other elements you deem relevant.

As we want to be able to compare answers across jurisdictions, we have drafted this request for information in a questionnaire format. This, however, does not mean we are looking for simple yes/no answers. Most questions are open questions and naturally invite an elaborate answer. Some questions may perhaps in theory be answered as yes/no question, but **please give as much guidance and details as possible within every question, to enhance our understanding of the legal system in your jurisdiction. Always cite the provision of the law or the case law you are relying on in providing an answer and please try to be exhaustive or at least as complete as possible. If you are relying on practical guidance or other informal rules and practice, please also refer to this and, if documentation on this is available, provide the link to where we can find this documentation.**

Please feel free to give additional guidance in the comments section at the end, in case you feel we did not sufficiently cover certain elements throughout the questionnaire.

formobile@netlaw.bg
Linkedin – Formobile-
Twitter – @Formobile2019
www.formobile-project.eu

The questionnaire is made up of 61 questions, in the following sections:

- ☐ Introductory questions
- ☐ Section 1: Criminal procedure when searching/reading mobile devices, seizing mobile devices and for acquisition of data on mobile devices
- ☐ Section 2: Criminal procedure rules on analysis of data from mobile devices
- ☐ Section 3: Admissibility of evidence before court
- ☐ Section 4: Interpretation and presentation of evidence from mobile forensics before the Court
- ☐ Section 5: Implications of the use of mobiles forensics on the role of the different parties in the trial
- ☐ Section 6: Comments

formobile@netlaw.bg
Linkedin – Formobile-
Twitter – @Formobile2019
www.formobile-project.eu

Introductory questions:

1. **Question:** *Please identify your organisation and your individual position?*

Answer: Dr. Mayeul Hiéramente, Fuhlrott Hiéramente & von der Meden Partnerschaft von Rechtsanwälten mbB (FHM), law firm specialized in Criminal Law and Labour Law. I am senior partner of the firm.

2. **Question**: *Where is your organisation based?*

Answer: Hamburg, Germany

3. **Question:** *Do you have a legally defined term for a "mobile device"? If yes, what kind of devices are included within it? (e.g. Smartphones, Tablets, Smartwatches, Cameras, MP3-players, Navigation devices, Drones)*

Answer: The German Code of Criminal Procedure (GCCP) does not contain any definition of a mobile device. The telecommunications act (GTA) defines only a telecommunication device (see section 3 (24a) GTA. Section 96 (1) No. 2 GTA refers to a "mobile connection" without providing any definition. In general, the provisions of the GCCP are deliberately formulated in a technologically neutral way so as to cover all relevant devices as well as possible new products.

formobile@netlaw.bg
Linkedin – Formobile-
Twitter – @Formobile2019
www.formobile-project.eu

Section 1: Criminal procedure when searching/reading mobile devices, seizing mobile devices and for acquisition of data on mobile devices

Question: *Mobile devices (e.g. a smartphone) may enter investigations in a variety of scenarios. A suspect or a witness may have a smartphone on them during questioning or at the scene, mobile devices may be found during the search of a home or other premises, a suspect caught in the act may have a mobile device in use etc. We want to know for all these scenarios (and others you may be able to identify) what the applicable national rules are, namely answering the following questions:*

Mobile device not seized

4. *Under what circumstances can a mobile device be read or searched without seizing it?*
5. *Are there any limits to this search (e.g. core area of private life, privacy limits, limits defined by the crime, limits defined by the order/warrant)? If so, how precise are these/must these be defined?*
6. *Is it allowed to use technical tools to bypass security?*
7. *Can information be copied or only read at this stage?*
8. *Is consent of the owner/person in possession of the mobile device necessary?*
9. *Can the owner/person in possession of the mobile device be forced to unlock the device?*
10. *Must the owner/person in possession of the mobile device be informed?*
11. *Who can order a search and what are the formal requirements, if any?*
12. *Does it matter whether this person is the accused or witness/third party or the victim?*
13. *What about data stored in the Cloud, what is the procedure to access/read this data if it is known or suspected to reside outside your jurisdiction? Is international cooperation like the European Investigation Order (hereinafter: EIO) or Mutual Legal Assistance Treaties (hereinafter: MLAT) the only route or do other options exist? Please elaborate.*
14. *Does any of the foregoing depend on the type of crime involved (e.g. terrorism, child pornography etc.)?*

formobile@netlaw.bg
Linkedin – Formobile-
Twitter – @Formobile2019
www.formobile-project.eu

15. *Does not following the applicable rules always lead to inadmissibility in court of the evidence in this scenario? If not, please elaborate on exceptions and relevant conditions.*

Answer to 4.-15.:

The legal regime applicable depends on whether the mobile device is used by the accused (see I.) or a third person (see II).

I. A mobile device used by the accused

The GCCP contains a multitude of provisions relevant for such situations. There is one set of provisions applicable to secret measures (see 1.) and another set of provisions that apply to open/transparent measures (see 2.)

1. Secret Measures

The GCCP knows multiple ways to read and/or copy data from a mobile device.

a. Section 100b GCCP (Covert remote search of information technology systems)

The most intrusive way to access data stored on a mobile device is via section 100b GCCP. The provision allows **secret access** to the device and the use of the technical means necessary to achieve such access. It permits **reading** as well as **copying** of the relevant data. It allows for access without the knowledge and consent of the accused. It would not require an EIO or MLAT as the data is accessed on the mobile device/at the source and therefore in Germany.

Such a covert remote search is limited to **particularly serious crimes** as listed in section 100b (2) GCCP. The provision is of **limited practical relevance** as it is, inter alia, require that the "technical means" are documented (see section 100b (4) in conjunction with section 100a (6) no. 1 GCCP.

It requires a written (see section 100e (3) GCCP with further formal requirements) **warrant** by the regional court (section 100e (2)) or the chamber president (in exigent circumstances). The prosecutor cannot decide on such measure in any circumstances. The warrant must describe the mobile device as detailed as possible (in practice this will e.g. be done by reference to the IMEI

number of a mobile phone). The warrant is limited to 3 months and can be renewed once. The operative part of the order shall indicate

1. the name and address of the person against whom the measure is directed, where known,

2. the alleged offence on the basis of which the measure is being ordered,

3. the type, extent, duration and end date of the measure,

4. the type of information to be obtained by carrying out the measure and its relevance for the proceedings,

[…]

6. in the case of measures under section 100b, as precise a designation as possible of the information technology system from which data are to be captured,"

If there are factual indications to assume that a measure will **only** lead to findings in the core area of the **private conduct of life**, the measure shall be inadmissible. Findings in the core area of the private conduct of life which are made on the basis of such measure may not be used. Recordings of such findings must be deleted without delay. The fact that such findings were made and their deletion shall be documented. Where possible in the case of measures under section 100b, technical means shall be employed to ensure that data concerning the core area of the private conduct of life are not captured (see section 100d GCCP).

Similar rules apply to any possible communication with individuals who have the right to refuse testimony on professional ground (section 53 GCCP), such as defence counsel, etc.

If the authorities decide to apply technical means to access the mobile device in a covert remote search they must ensure that technical means are in place so that only those changes are made to the information technology system which are essential in order to capture the data; and the changes made are automatically reversed once the measure is concluded, insofar as this is technically possible. The means used shall provide **protection against unauthorised access using methods**

formobile@netlaw.bg
Linkedin – Formobile-
Twitter – @Formobile2019
www.formobile-project.eu

reflecting the state of the art. Copied data shall be protected against modification, unauthorised deletion and authorised inspection using methods reflecting the state of the art. (section 100b (4) in conjunction with section 100a (5) GCCP).

Note: This is the only provision in the GCCP that addresses the issue of data authenticity.

Furthermore, section 100b (4) in conjunction with section 100a (6) GCCP requires documentation.

The provision, however, does not address the issue of admissibility of evidence that has not been properly protected against modification. The issue has not been addressed by the courts either. It is, however, extremely unlikely that evidence would be declared inadmissible for such reason.

For further information see sections 100b, 100d, 100e GCCP that describe the requirements and procedures in detail.

The measure does not require consent of the accused. The targeted person needs to be notified (section 101 (4) no. 4 GCCP). Mention is to be made in the notification of the option of subsequent legal protection pursuant to section 101 (7) and of the applicable time limit. Such notification can be postponed if notification would endanger the investigations (section 101 (5) GCCP) The reasons must be documented. If notification is deferred pursuant to section 101 (5) GCCP and has not been given within 12 months after completion of the measure, any further deferral of notification shall be subject to the approval of the court. The court shall decide 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.

Decisions and other documentation concerning measures under section 100b GCCP shall be deposited at the public prosecution office. They shall be added to the files only if the conditions concerning notification under section 101 (5) GCCP are met. Personal data which were collected by means of measures under section 100b GCCP are to be labelled accordingly. Following transfer of the data to another agency, the labelling is to be maintained by such agency.

formobile@netlaw.bg
Linkedin – Formobile-
Twitter – @Formobile2019
www.formobile-project.eu

Regarding **admissibility of evidence**:

Findings in the **core area of the private conduct of life** which are made on the basis of a measure under sections 100a to 100c may not be used (section 100d (2) GCCP). The same applies to measures infringing on the protected communication with individuals who have the right to refuse testimony on professional ground (section 53 GCCP). In section 100d (5) s. 2 GCCP the law provides that information by a relative in the sense of section 52 GCCP (e.g. children, parents) can be inadmissible if the use of such information is disproportionate. Very personal information in a "digital diary" can also be considered inadmissible (Bader/KK-StPO, 8. ed. 2019, Vor § 48, para. 37).

Violations of the procedural rules can lead to inadmissibility. Given the jurisprudence of the German courts regarding other investigative measures it seems clear that a covert remote **search** of a mobile device **without a warrant** by a judge/court will lead to the inadmissibility of the evidence gathered by such search (Köhler/Meyer-Goßner/Schmitt, 62. Aufl. 2019, § 100b, para. 15).

b. Section 100a GCCP (Telecommunications surveillance)

Section 100a GCCP allows for the **secret** surveillance of telecommunication. It also applies to mobile devices such as smartphones. The provision allows for a surveillance order regarding the device itself (**IMEI**-number of the device) and/or the **SIM**-card used in the device. It allows for a direct surveillance by the authorities or – the standard case in practice – an indirect surveillance via a cooperation request to a provider of publicly accessible telecommunications services. A telecommunication surveillance under section 100a GCCP permits **listening/reading** as well as **copying** of telecommunication data.

Telecommunication surveillance requires, in general, a **written warrant** by the local **court** (investigative judge). In exigent circumstances, the public prosecution office may also make the order (section 100e (1) GCCP). The order shall be limited to a maximum duration of three months. An extension of no more than three months in each case shall be admissible if, taking into account

the information obtained in the course of the investigation, the conditions for the order continue to exist. The written warrant must contain the following information:

1. the name and address of the person against whom the measure is directed, where known,

2. the alleged offence on the basis of which the measure is being ordered,

3. the type, extent, duration and end date of the measure,

4. the type of information to be obtained by carrying out the measure and its relevance for the proceedings,

5. in the case of measures under section 100a, the telephone number or another identifier of the connection to be intercepted or the end device, insofar as certain facts do not lead to the assumption that it is assigned to another end device; in the case under section 100a (1) sentences 2 and 3, as precise a designation as possible of the information technology system to be interfered with, […].”

Such measures are only permitted with regards to **serious crimes** as listed in section 100a (2) GCCP. The judge must establish “certain facts” that give rise to the suspicion that such crimes have been committed and the offence is one of particular severity in the individual case as well. The German Constitutional Court (BVerfG, 27.5.2020, 1 BvR 1873/13 et al.) has stated that the **evidentiary standard** of “certain facts” is higher than the threshold for launching a criminal investigation (“sufficient factual indications, see section 152 (2) GCCP).

The provision allows to intercept and record “telecommunication”. The legal definition of the term is, however, not entirely clear. It certainly applies to calls, text messages, chats (e.g. whatsapp and Skype), e-mails, social media activities, etc. There is an ongoing and controversial debate whether the provision also allows interception and recording of **data transfers** that lack the aspect of **social interaction**.

A first debate concerns the question whether the ongoing use of internet browsers (“**surfing the internet**”) can be reviewed under section 100a GCCP. While many authors consider such use of the internet as outside the scope of section 100a GCP (Hiéramente, HRRS 2016, 418; Schmitt, in:

formobile@netlaw.bg
Linkedin – Formobile-
Twitter – @Formobile2019
www.formobile-project.eu

Meyer-Goßner/Schmitt, StPO, § 100a Rn. 7d; Wolter/Greco, in: SK-StPO, 5. Aufl. (2016), § 100a Rn. 31a; Albrecht/Braun HRRS 2013, 500, 502; Meinicke DSRITB 2013, 967, 970 f.; Braun jurisPR-ITR 18/2013 Anm. 5; Albrecht, jurisPR-ITR 14/2013 Anm. 4; Sieber, Straftaten und Strafverfolgung im Internet (2012), C 107; Bosbach, Verteidigung im Ermittlungsverfahren, 8. ed. (2015), p. 35), the Regional Court of Ellwangen decided that 100a GCCP applies (LG Ellwangen, 28.5.2013 – 1 Qs 130/12). The decision by the Regional Court Ellwangen was declared constitutional by the German Constitutional Court (BVerfG, 6.7.2016, 2 BvR 1454/13).

This led to a second debate that is of more direct relevance to the present case. It is subject to intense debate whether section 100a GCCP allows the authorities to intercept and record the **data transfer between a mobile device and the cloud.** The courts have not yet addressed this issue and the majority of authors consider section 100a GGCP not to be applicable as they consider such (automatic) transfer of data as something inherently different than the "classical" form of telecommunication (Roggan StV 2017, 821 (823); Köhler/Meyer-Goßner/Schmitt, 62 ed. 2019, § 100a, Rn. 14 f; Wolter/Greco/SK-StPO, 5. ed. 2016, § 100a, Rn. 41; Hiéramente/Fenina StraFo 2015, 365; Sieber, „Straftaten und Strafverfolgung im Internet", Expert Opinion to the 69. DJT, 2012, C- 106 ff.; Sieber/Brodowski, in: Hoeren/Sieber/Holznagel, Multimedia-Recht, 50. EL 2019, Teil 19.3, Rn. 135; Expert Opinion for the German Parliament BT-Drs. 18/11272, see: https://www.bundestag.de/resource/blob/506900/ee10356f95642a80b0b8cf81d22c5d6c/sinn-data.pdf;; for a contrary view see Bruns, KK-StPO, 8 ed. 2019, § 100a, para. 4; Singelnstein/Derin, NJW 2017, 2646). So far, there has been **no jurisprudence** in this regard and also **no clear decision by the German legislature**. The authors opposing an application of section 100a GCCP mostly consider that such measures should only be permitted if the conditions set out in section 100b GCCP ("very serious crimes") are met. If one were to allow such measures, it would not require an EIO or MLAT as the data is accessed on the mobile device/at the source and therefore in Germany.

Section 100a (1) s. 2, 3 GCCP also allows the use of technical means to allow such surveillance (e.g. in the case of **encrypted** communication):

formobile@netlaw.bg
Linkedin – Formobile-
Twitter – @Formobile2019
www.formobile-project.eu

"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."

While the "normal" procedure requires cooperation from the provider of publicly accessible telecommunications services and only allows the collection of (at times encrypted) data during transfer ("transport encryption"), interception under this sub-section (called Quellen-TKÜ = surveillance at the source") allows the authorities to **access the mobile device** and retrieve the data before it is encrypted. It is important to note, however, that the provision only allows the recording of **"ongoing" telecommunication.** The provision states very clearly that that is has to be ensured by technical means that the content and circumstances of the communication which could also have been intercepted and recorded **from the date on which the order was made** pursuant to section 100e (1). This means for example that the authorities are not authorized to access emails or text messages that have been exchanged prior to the warrant. The provision also states: "*The content and the circumstances of the communication stored in the person concerned's information technology systems may be intercepted and recorded if they could also have been intercepted and recorded in encrypted form during ongoing transmission processes in the public telecommunications network.*" This also means that it is not permitted to surveil the **drafting** of a message if such message is not subsequently sent.

If the authorities decide to apply technical means to access the mobile device for telecommunication surveillance they must ensure that technical means are in place so that only those changes are made to the information technology system which are essential in order to capture the data; and the changes made are automatically reversed once the measure is concluded, insofar as this is technically possible. The means used shall provide **protection against unauthorised access using methods reflecting the state of the art. Copied data shall be protected against modification, unauthorised deletion and authorised inspection using methods reflecting the state of the art**. (section 100a (5) GCCP). Section 100a (6) GCCP requires additional documentation of the investigative measure.

formobile@netlaw.bg
Linkedin – Formobile-
Twitter – @Formobile2019
www.formobile-project.eu

Section 100d GCCP (see also below) contains rules to protect the accused from measures intruding in his private life and to protect the communication with individuals who have the right to refuse testimony on professional ground (section 53 GCCP), such as defence counsel, etc.

The measure does not require **consent** of the accused. The targeted person needs to be notified (section 101 (4) no. 3 GCCP). Such **notification** can be postponed if such notification would endanger the purpose of the investigation, the life, physical integrity and personal liberty of another or significant assets, in the case under section 110a including the possibility of the continued use of the undercover investigator (section 101 (5)). The reasons must be documented. Other participants have to be notified. Mention is to be made in the notification of the option of subsequent legal protection pursuant to section 101 (7) and of the applicable time limit. If notification is deferred pursuant to section 101 (5) GCCP and has not been given within 12 months after completion of the measure, any further deferral of notification shall be subject to the approval of the court. The court shall decide 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.

Notification of such persons whoe were not the target of the measure may be dispensed with if such persons were only tangentially affected by the measure and it may be assumed that the person has no interest in being notified. Personal data which were collected by means of measures under section 100a GCCP are to be labelled accordingly. Following transfer of the data to another agency, the labelling is to be maintained by such agency.

Regarding the **admissibility of evidence**:

Findings in the core area of the **private conduct of life** which are made on the basis of a measure under sections 100a to 100c may not be used (section 100d (2) GCCP). Section 160a (1) s. 2 GCCP proclaims that information exchanged between the accused and e.g. an **attorney** cannot be used for the investigation (see also Köhler/Meyer-Goßner/Schmitt, 62. ed. 2019, § 160a, para. 4). The provision refers to section 53 (1) s. 1 no. 1, 2, 4 GCCP.

formobile@netlaw.bg
Linkedin – Formobile-
Twitter – @Formobile2019
www.formobile-project.eu

Violations of (important) **procedural rules** can lead to the inadmissibility of the evidence. This requires a sufficiently grave violation. This is generally the case when the responsibility of the judge (or prosecutor) to order such a measure has been ignored (see e.g. BGH, Judgment 17.3.1983 – 4 StR 640/82), when there was no allegation of a serious crime (BGH, Judgment 17.3.1983 – 4 StR 640/82), when information collected is used for the prosecution of an unrelated offense lacking the seriousness as determined in section 100a (2) GCCP (BGH, Judgment, 30.8.1978 – 3 StR 255/78). Whether or not the surveillance will be an efficient tool to collect evidence and therefore needed for the investigation is subject to uncertainties so that there is generally no reason to consider evidence resulting from such a measure as inadmissible. Same applies to an appellate review of the factual assessment by the local court judge regarding the "certain facts" (see BGH, Judgement, 16.2.1995 – 4 StR729/94). Data collected via a surveillance at the source that dates before the relevant warrant is most likely also to be considered as inadmissible (Köhler/Meyer-Goßner/Schmitt, 62. ed. 2019, § 100a, para. 35a).

c. Section 100g (Traffic data capture) and other measures

Section 100g GCCP allows for a request to the provider of publicly accessible telecommunications services and permits access to **traffic data** stored by the provider for private or public purposes. It does not allow access to data stored **on the device** and does therefore not fall under the scope of this questionnaire. Same holds true for a "**silent SMS**" sent to the mobile device to produce traffic data for a search for the device/accused or the use of the **IMSI-Catcher**. Both methods (see section 100i GCCP) do not allow the authorities to access data stored on the mobile device.

2. Open/Transparent Measures

The GCCP allows for different open/transparent measures.

a. Section 94: Seizing of data at the provider level

Section 94 GCCP states:

formobile@netlaw.bg
Linkedin – Formobile-
Twitter – @Formobile2019
www.formobile-project.eu

(1) Objects which may be of importance, as evidence, for the investigation shall be taken into custody or otherwise secured.

(2) Such objects shall be seized if they are in the custody of a person and are not surrendered voluntarily.

The German Constitutional Court held that the provision **also applies to data** despite the use of the term "object" (BVerfG, 12.4.2005 – 2 BvR 1027/02). The German Constitutional Court also held that the provision allows for an investigative measure that affects the constitutional right of secrecy of communications (article 10 GG). It is therefore permitted under section 94 GCCP to seize **emails** stored with the (German) provider as long as such measures are proportionate (BVerfG, Judgement, 6.6.2009 – 2 BvR 902/06). The conditions set out in section 100a GCCP do not have to be satisfied (BVerfG, Judgement, 6.6.2009 – 2 BvR 902/06). Same applies to traffic data (see section 100g (5) GCCP).

The Federal Court of Justice clarified that section 94 GCCP is an open/transparent investigative measure and therefore requires an **immediate notification** to the person to whom the seized data belongs (BGH, 24.11.2009 – StB 48/09 a)). The seizing of data saved by the provider is not a permanent measure. It only allows access to the data saved at the moment of the order (BVerfG, Judgement, 6.6.2009 – 2 BvR 902/06).

A seizure is generally **ordered by a judge.** In exigent circumstances it can be ordered by a prosecutor or the investigators (section 98 GCCP). A seizure can only be ordered if the relevant data has a potential evidentiary value. If this cannot be ascertained, the authorities will have to request **a search warrant** and must make a cursory review of the relevant data before ordering the seizure of the selected data (BVerfG, Judgement, 6.6.2009 – 2 BvR 902/06; BVerfG, 12.4.2005 – 2 BvR 1027/02). A search warrant is also issued by a judge but can be ordered by the prosecutor or investigator in exigent circumstances (section 105 (1) GCCP).

If the accused grants access to the data, a warrant is not required. A seizure does not require any consent of the parties involved.

If the authorities merely intend to access the data – without being in possession of the mobile device – stored with the provider/in the cloud, they can issue a cooperation request (section 95 GCCP) – if the evidentiary relevance is clear – or a search warrant (sections 103, 105 GCCP) for the servers – if the content is not entirely clear – used for storage by the provider. If the server/cloud is situated outside Germany, an EIO or a MLAT is required (for the Cybercrime Convention see below).

b. Section 102 GCCP: Search of mobile device

The authorities can decide to **search the mobile device** in possession of the accused.

(1) Search of device

Such a measure is based on section 102 GCCP and requires a search warrant that is normally issued by a **judge**. In exigent circumstances it can be ordered by a prosecutor or the investigators (section 105 (1) GCCP). While the order must not necessarily be in writing, it is necessary that the authorities provide for **written documentation** of the decision in order to allow for a subsequent judicial review of the warrant (BVerfG, 23.7.2007 – 2 BvR 2267/06).

The accused has the right to be present at the search (section 106 (1) s. 1 GCCP). If he is absent, his representative, an adult relative, a person living in his household or a neighbour shall, if possible, be called in to assist. Since the accused will normally not be heard before the warrant is issued (section 33 (4) GCCP) he will be notified of the decision after the search (see also sections 35, 107 GCCP).

The accused can request documentation regarding the search and possible seizures. The prosecutor is allowed to review the seized mobile device (section 110 (1) GCCP). It can allow its investigators to do the review. The investigators are also permitted to do the review if approved by the accused (section 110 (2) GCCP). Sections 102, 110 (1), (2) GCCP allow the authorities to **read** the data. If they want to **copy/safe** the data for use in the ongoing criminal proceedings they have to either seize the mobile device or the data stored on the device (section 94 GCCP). This clear division between the search on the one and the seizure on the other hand notwithstanding, the courts have developed a status in between which they refer to as **"preliminary seizure"** (BVerfG, 12.4.2005 -

formobile@netlaw.bg
Linkedin – Formobile-
Twitter – @Formobile2019
www.formobile-project.eu

2 BvR 1027/02). It has been developed with regards to searches of premises but should also apply to the search of objects. The jurisprudence takes into consideration the fact that a search can take a long time and could therefore be disproportionate. It also notes that it would be disproportionate to seize an entire mobile device and keep such a device in police custody for the remaining proceedings. The German Constitutional Court accepts the concept of "preliminary seizure" as part of the search. It permits the authorities to either take the mobile device for further screening or to prepare a forensic image which can be screened (with the advantage that the owner can use the original). In such circumstances the authorities are **entitled to copy data before a formal seizure** of the device or the data contained therein. It is subject to intense discussion whether the owner of the device/data is allowed to be present during such screening (contra Michalke, StraFo 2014, 89; Heuel/Beyer, AO-StB 2011, 245, 247; Knauer/Wolf, NJW 2004, 2932, 2937 f.; Gercke, in: HK-StPO, 5. ed. 2012, § 110, para. 13, Hiéramente, wistra 2016, 432, pro: LG Bonn, v. 23.8.2011, 27 Qs 17/11 (in an anti-trust case and not a criminal case); Hauschild, in: MüKo-StPO, 1. Ed. 2014, § 110, para. 14; Saller, CCZ 2012, 189, 192).

The GCCP does not contain any explicit provisions regarding the **admissibility** of evidence gathered through the search of a mobile device. Sections 97, 148 160a (1) GCCP contain certain limitations as to the admissibility of evidence obtained in violation of legal privilege. The courts also acknowledge that serious violations of procedural rules can lead to inadmissibility of the evidence gathered through a search. Searches without proper warrant or an inappropriate determination of "exigent circumstances" can lead to inadmissibility (see e.g. BGH, 30.8.2011 – 3 StR 210/11). The German Constitutional Court clarified that "exigent circumstances" can normally not be claimed once the judge has received the request for the judicial warrant (BVerfG, 16.6.2015 - 2 BvR 2718/10 et al.). The provision does not contain any explicit limits with regard to the protection of private life. The courts have, however, recognized that the constitution requires the protection of a core of private life even in cases of searches and seizures (see BGH, Judgement, 9.7.1987 – 4 StR 223/87). A protection of such data can lead to its inadmissibility.

(2) Access to cloud

formobile@netlaw.bg
Linkedin – Formobile-
Twitter – @Formobile2019
www.formobile-project.eu

Once a search is granted under sections 102, 105 GCCP the authorities are also permitted to access the cloud. Section 110 (3) GCCP stipulates:

"The examination of an electronic storage medium on the premises of the person affected by the search may be extended to also cover physically separate storage media insofar as they are accessible from the storage medium if there is a concern that the data sought would otherwise be lost. Data which may be of significance for the investigation may be ***secured*** *[…]."* [Please note that the term 'premises' used in the official translation of the GCCP is not included in the original]

If the authorities secure data from the cloud, they have to follow the procedure laid down in section 98 (2) GCCP which itself only applies to the seizure of objects and which states:

"An official who has seized an object without a court order is, as a rule, to apply for court confirmation ***within three days*** *if neither the person concerned nor an adult relative was present at the time of seizure or if the person concerned and, if he was absent, an adult relative of that person expressly objected to the seizure."*

While there has been no jurisprudence in this regard, there is widespread agreement that section 102 in conjunction with section 110 (3) GCCP only allows access to a separate storage medium within the boundaries of the Federal Republic of Germany (Bär, Handbuch Wirtschafts- und Steuerstrafrecht, 4. Ed. 2014, 27 B. Rn. 27; Warken, NZWiSt 2017, 329, 338; Hauschild, MüKo-StPO, 1. Ed. 2014, § 110, para. 18). A **direct access** to a server in a foreign country would be an illegal **infringement on the sovereignty** of the country in which the data is stored. Direct access can, however, be permitted with the permission of the accused (see Article 32b of the Cybercrime-Convention). Without the permission of the accused the authorities can request cooperation under different cooperation regimes that also allow for a quick-freeze-solution. In Germany the following cooperation regimes are considered most relevant: Cybercrime-Convention, Council Framework Decision 2003/577/JHA of 22 July 2003 on the execution in the European Union of orders freezing property or evidence; analogous application of article 20 (4) Convention established by the Council in accordance with Article 34 of the Treaty on European Union, on Mutual Assistance in Criminal

Matters between the Member States of the European Union (see Hauschild, MüKo-StPO, 1. Ed. 2014, § 110, para. 18).

The courts have not yet decided whether an illegal direct access leads to the **inadmissibility** of the evidence. Most commentators are doubtful in this regard since inadmissibility is the exception and requires a significant violation of the procedures in place. Furthermore, the main argument is one that is not meant to protect the interests of the accused (Hauschild, MüKo-StPO, 1. Ed. 2014, § 110, para. 19 with further references). The Federal Court of Justice has, however, declared evidence gathered in violation of the sovereignty of another State as inadmissible in a case where the other State has objected to the use of the evidence in question (BGH, Judgment, 8.4.1987 – 3 StR 11/87).

(3) Password, fingerprints/face-recognition, brute force

The accused **can refuse** to provide the authorities with the password.

The authorities might, however, be able to rely on other sources. Section 100j (1) s. 2 GCCP stipulates:

"If the request for information under sentence 1 refers to data by means of which access to terminal equipment or to storage media installed in such terminal equipment or physically separate therefrom are protected (section 113 (1) sentence 2 of the Telecommunications Act), information may only be requested if the statutory requirements for the use of such data are met."

By virtue of this provision, the authorities can request from the provider of publicly accessible telecommunications services the **PIN** and **PUK** to a SIM-card used by the accused. The Federal Constitutional Court has also stated that such a request for information will – under normal circumstances – not cover the password set by the client to unlock the mobile device because such information is not kept in an unencrypted way (see BVerfG, 27.5.2020 – 1 BvR 1873/13 et al). Furthermore, such a request can only be addressed to a "provider of publicly accessible **telecommunications**" and **not** to App developers, hardware producers (see also Hiéramente/Pfister, StV 2017, 477), etc. An order under section 100j (1) s. 2 GCCP would normally require a warrant (section 100j (3) s. 1 GGCP). Such a warrant is, however, not necessary if the

data subject – here the accused – already has or must have knowledge of the request for information or if the use of the data has already been permitted by a court decision (e.g. a search warrant). The data subject shall be **notified** of the request for information. Notification shall take place insofar as and as soon as this can be effected without thwarting the purpose of the information. It shall be dispensed with where overriding interests meriting protection of third parties or of the data subject himself constitute an obstacle thereto. Where notification is deferred the reasons therefor shall be documented.

Therefore, it is generally not possible to get hold of the password of the mobile device used by the accused to lock/unlock the mobile device. There is an ongoing discussion whether the authorities are allowed to use the **fingerprints** of the accused and/or **face recognition** to unlock a mobile device (if the user activated such an option on his/her phone). There is no jurisprudence in this regard and no legal provision addressing this specific question. It is argued by some authors that **section 81b GCCP** can be used to access a phone by using the fingerprints of the accused (Rottmeier/Eckel, NStZ 2020, 193; Bäumerisch, NJW 2017, 2718; for a contrary view see Momsen DRiZ 2018, 140, 141; Nadeborn/Irscheid StraFo 2019, 274, 275; Horn Krim 2019, 641, 642; Sieber/Brodowski, in: Hoeren/Sieber, Multimedia-Recht, April 2020, 19.3, para. 196). The provision states:

*"Photographs and **fingerprints** of the accused may be taken, even against his will, and measurements may be made of him and other similar measures taken with regard to him insofar as is required **for the purposes of conducting the criminal proceedings** or of the police records department."*

A similar view is held with regards to face recognition. The authors approving of such a measure highlight that section 81b GCCP only allows the access to the mobile device and not the review or seizure of the data on the device. This requires (see above) a separate legal basis (Rottmeier/Eckel, NStZ 2020, 193). Given the previous jurisprudence of the German Constitutional Court (BVerfG, 24.1.2012 – 1 BvR 1299/05 regarding passwords saved by the provider) it should be a

constitutional prerequisite that the (formal) conditions for the use of the data on the mobile device are met **before** allowing any application of section 81b GCCP.

So far there is **no jurisprudence** on this regard. It remains to be seen whether the right not to have to self-incriminate forbids the application of section 81b GCCP (for a contrary view see Rottmeier/Eckel, NStZ 2020, 193 who state that the provision does not require an "active" participation of the accused). Furthermore, it remains to be seen if the German Constitutional Court would tolerate the broad definition of section 81b GCCP as it might not guarantee that restrictions for the use of the data are also taken into consideration at the "first level". In a different case (BVerfG, 27.5.2020, 1 BvR 1873/13 et al.) the German Constitutional Court has determined that relevant restrictions must be taken into consideration in the wording of the provisions for both levels of a data transfer. Finally, it has been argued that any circumvention of the procedural rules set out in section 100j (3) GCCP is problematic (Sieber, Straftaten und Strafverfolgung im Internet, 2012, C 9, 121. Graf, in: BeckOK StPO, 37. Ed. July 2020, § 100j, para. 18, for another view see Rottmeier/Eckel, NStZ 2020, 193). This aspect should be of minor relevance since the intended search under section 102 GCCP already requires a warrant so that the – possible – circumvention of section 100j (3) GCCP does not apply to this particular case.

The authorities are also entitled to use **technical means to "hack" the mobile device** (Zerbes/El-Ghazi, NStZ 2015, 425; Hauschild, in: MüKo-StPO, 2014, § 105, para. 31 with further references; Obenhaus NJW 2010, 651). While there is no explicit jurisprudence it has been recognized by courts that a search warrant also allows a proportionate use of force to access the premises (OLG Stuttgart, 13.10.1983 – 3 Ss 535/83

Such measures are, however, very time-consuming and depending on the level of encryption (see Bäumerich NJW 2017, 2718) not a realistic option for investigators in most cases. It is subject to debate whether the use of technical means is also permitted to bypass a password used to protect access to the cloud from the mobile device since section 110 (3) GCCP grants access to the cloud only "*insofar as they are **accessible** from the storage medium*" (against the use of "brute force"

formobile@netlaw.bg
Linkedin – Formobile-
Twitter – @Formobile2019
www.formobile-project.eu

Brodowski/Eisenmenger, ZD 2014, 119; for such use see Obenhaus NJW 2010, 651; Hegmann, BeckOK StPO, 2020, § 1110, para. 17).

II. A mobile device used by a third person / witness

The rules that apply to mobile devices used by a third person / witness differ from those applicable to the accused.

1. Secret Measures

The GCCP also allows for secret measures in certain cases.

a. Section 100b GCCP (Covert remote search of information technology systems)

For the explanation of the provision, see above. A measure may only target mobile devices by third persons in exceptional circumstances. Section 100b (3) s. 2 GCCP states:

"*Interference with the information technology systems of other persons shall be permissible only where it is to be assumed, on the basis of certain facts, that*

1. the accused designated in the order made pursuant to section 100e (3) uses the other person's information technology systems and

2. 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."

b. Section 100a GCCP (Telecommunications surveillance)

For the explanation of the provision, see above. Section 100a (3) GCCP states:

"Such order may be made only against the accused or against persons in respect of whom it may be assumed, on the basis of certain facts, that they are receiving or transmitting messages intended for or originating from the accused, or that the accused is using their telephone connection or information technology system."

formobile@netlaw.bg
Linkedin – Formobile-
Twitter – @Formobile2019
www.formobile-project.eu

c. Section 100g (Traffic data capture) and other measures

Sections 100g GCCP and 100i GCCP focus on the accused and do not apply to mere witnesses.

2. Open/Transparent Measures

The GCCP allows for different open/transparent measures.

a. Section 94: Seizing of data at the provider level

For the explanation of the provision, see above. Section 94 GCCP does not differentiate between the accused or third persons. Therefore, it is possible – in theory – that the authorities seize the (online) email account or other data stored with a (German) provider belonging to a person other than the accused. It will, however, be much more difficult to determine (before having reviewed the data) that the data "*may be of importance, as evidence, for the investigation*". If the authorities believe that relevant might be stored at the provider level, they can request a search warrant (see below). Since they intend to screen data belonging to a person other than the accused, a search warrant can only be granted if the conditions set out in section 103 GCCP are fulfilled. This provision requires:

"Searches in respect of other persons shall be admissible only for the purpose of apprehending the accused or to follow up the traces of an offence or ***to seize certain objects*** *and only if* ***certain facts support the conclusion*** *that the person, trace or object sought is located on the premises to be searched. […]"*

Under normal circumstances, such a **warrant** needs to be issued by the local court (section 105 GCCP). The German Constitutional Court states that "certain facts" require a higher evidentiary standard than the standard to initiate a criminal investigation (BVerfG, 27.5.2020, 1 BvR 1873/13 et al). The German Constitutional Court allows, however, that the judge indicates categories of objects to satisfy the "certain objects" standard (BVerfG, 28.4.2003 – 2 BvR 358/03). Individual courts have asked for additional guidelines for the search by the judge (see e.g. LG Itzehoe,

formobile@netlaw.bg
Linkedin – Formobile-
Twitter – @Formobile2019
www.formobile-project.eu

12.1.2015 - 2 Qs 162-164/14) to guarantee that the limits set out in section 103 GCCP are abided by in practice.

b. Section 103 GCCP: Search of mobile device

The authorities can decide to **search the mobile device** in possession of a third person.

(1) Search of device

For the description of section 103 GCCP, see above. The authorities can search the mobile device of a person other than the accused if the (slightly) stricter conditions of section 103 GCCP are met. Such searches **do not require the consent** of the owner/person in possession.

A "**preliminary seizure**" (see above) is also possible in a search based on a warrant pursuant to section 103 GCCP. It is even a more common occurrence since section 103 GCCP requires a more careful assessment of the (possible) evidence to avoid a disproportionate seizure of devices and data.

Since the person will normally not be heard before the warrant is issued (section 33 (4) GCCP) he/she will be notified of the decision after the search (see also sections 35, 107 GCCP).

(2) Access to cloud

The GCCP also permits **access to the cloud through the mobile device** that is subject to the search warrant (sections 103, 110 (3) GCCP). Such a screening of data on the cloud has to respect the limits set out in section 103 GCCP as well as in the (written) search warrant. Section 110 (3) GCCP contains one additional limit that the authorities tend to ignore in practice but is relevant when the authorities access the cloud via a mobile device not belonging to the accused. The provision only permits (direct) access to the cloud "*if there is a concern that the data sought would otherwise be lost".*

(3) Password, fingerprints/face-recognition, brute force

If the mobile device belongs to a person other than the accused, the rules differ with regards to passwords.

formobile@netlaw.bg
Linkedin – Formobile-
Twitter – @Formobile2019
www.formobile-project.eu

Section 100j GCCP also applies to the situation but only makes access to PIN and PUK possible (see above). While it is not entirely clear from the existing case law, it seems that the authorities can request **cooperation from a witness** in the form of testimony (sections 48 et seq. GCCP) – if the password is not written down – or an order to produce evidence (section 95 GCCP) – if the password is written down. While there are good reasons to doubt whether such information, which is meant (merely) to help the investigation, is "evidence" in the sense of these provisions (see Hiéramente/Graßie, CB 2019, 191), a regional court has acknowledged a civic duty to cooperate in such cases (see LG Trier, 16.10.2003, 5 Qs 133/03). Witnesses can refuse testimony and/or cooperation with a request in the sense of section 95 GCCP in the following situations:

- Section 52 GCCP (relatives of the accused)
- Section 53 GCCP (legal privilege)
- Section 55 GCCP (for the application with regards to requests pursuant to section 95 GCCP see Menges, in: Löwe-Rosenberg, 27. Aufl., 2018, § 95, Rn. 16; Wohlers/Greco, in: SK-StPO, 5. Aufl. 2016, § 95, Rn. 21), which states:

  (1) Any witness may refuse to answer any questions the reply to which would subject him or one of the relatives indicated in section 52 (1) to the risk of being prosecuted for an offence or a regulatory offence.
  (2) The witness shall be instructed as to his right to refuse to answer.

Section 81b GCCP only applies to the accused and does not entitle the authorities to take the **fingerprints** of a third person. Section 81c GCCP, which refers to the examination of other persons, does not apply to this particular case.

If the witness refuses to cooperate, the authorities may use technical means (see above).

formobile@netlaw.bg
Linkedin – Formobile-
Twitter – @Formobile2019
www.formobile-project.eu

Mobile device seized

16. *Can the mobile device (e.g. a smartphone) be seized?*

Yes. A mobile device can be seized pursuant to section 94 GCCP. The provision can be applied to a mobile device belonging to an accused as well as one belonging to a third person.

17. *What are the conditions for this, who can order it and what are the formal requirements?*

The conditions are set out in **sections 94, 98 GCCP**. Section 97 contains limits to a seizure due to legal privilege. A seizure requires the assessment that the mobile device **may be of importance**, as evidence, for the investigation. The German Constitutional Court has clarified that the authorities must, before seizing a (mobile) device, attempt to determine whether the entire data stored on the device is relevant for the proceedings (BVerfG, 12. 4. 2005 - 2 BvR 1027/02). This is especially important if the device belongs to a person other than the accused. There is, however, no clear-cut rule that determines under which circumstances a prior review of the content is required. If the device is encrypted and the authorities have reason to believe that it contains evidence, the seizure of the mobile device is most likely permitted. A seizure order needs to take into consideration that such a measure also affects the telecommunication secrecy (BVerfG, 4.2.2005 – 2 BvR 308/04).

A seizure is required if the person in possession of the device did not surrender the device voluntarily. It must normally be **ordered by a judge** (investigative judge), see 98 (1) GCCP. in exigent circumstances it can be ordered by the public prosecution office and its investigators. The provision, recognizing the relevance of a seizure, contains an additional safeguard in section 98 (2) GCCP:

"An official who has seized an object without a court order is, as a rule, to apply for court confirmation within three days if neither the person concerned nor an adult relative was present at the time of seizure or if the person concerned and, if he was absent, an adult relative of that

person expressly objected to the seizure. The person concerned may at any time apply for a court decision."

18. *If seized, can the mobile device always be searched, information copied etc?*

Once the mobile device has been seized it can be searched and information can be copied. Excluded from any use is information covered by legal privilege as defined in sections 97, 148 GCCP. Since it is generally required that a screening or search occurs before a mobile device is seized – to avoid seizure of irrelevant and sensible data – there are few practical limitations to the use of information contained in the device.

19. *Are there any limits to this search (e.g. core area of private life, privacy limits, limits defined by the crime, limits defined by the order/warrant)? If so, how precise are these/must these be defined?*

Generally speaking, there are no limits to a search of a device already seized. The selection should normally take place before the seizure. This notwithstanding, the authorities continue to be bound by limits such as legal privilege or the core area of the private conduct of life. Furthermore, section 500 GCCP refers to the Federal Data Protection Act which contains as a basic principle that "*personal data shall be 1. processed lawfully and fairly; 2. collected for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes"*

If the mobile device is seized under section 94 GCCP, the (category) of crime is not relevant for the use of the data. In contrast, the use of data gathered through investigative measures such as telecommunications surveillance or covert remote search of information technology systems is restricted to certain types of (very) serious crimes.

formobile@netlaw.bg
Linkedin – Formobile-
Twitter – @Formobile2019
www.formobile-project.eu

A warrant pursuant to section 94 GCCP only defines which objects are seized and not the possible investigations in this regard. A search warrant, on the other hand, is subject to limitations (purpose, objects, timeframe, etc.) that the court is tasked with to define.

20. *Is consent of the owner/person in possession of the mobile device ever a relevant element?*

In general, consent of the owner is not required if the judge orders a seizure. Nonetheless, the person can always consent to its use.

21. *Can the owner/person in possession of the mobile device (if identified) be forced to unlock the device?*

The **accused** cannot be forced to unlock the device. Some authors consider that his fingerprints as well as face recognition can be used. (see above)

A witness is – with some exceptions – obliged to provide the password. A witness cannot be forced to unlock the device him- or herself (see above). The fingerprints cannot be used.

22. *Must the owner/person in possession of the mobile device be informed? If so, about what exactly?*

The owner/person in possession must be informed of a search (see above). If the authorities request a seizure by the local court judge, section 33 (3) GCCP grants the owner/person in possession the right to be heard in order to allow him to advance factual and legal arguments. The owner/person in possession must be informed about the objects the authorities want to seize as well as about the statements of the prosecutor in such proceedings.

23. *Is it allowed to use technical tools to bypass security measures and/or anti-forensic measures?*

Most authors considered it permissible to bypass security measures and/or anti-forensic measures as part of the search and seizure (see above).

24. *Does it matter whether this person is the accused or witness/third party or the victim?*

Generally speaking, section 94 GCCP does not differentiate between the accused or witness/third party or the victim. Every measure must, however, be proportionate. The authorities will therefore, *inter alia*, have to try to receive cooperation from a witness/victim before trying to "hack" the mobile device.

25. *What about data stored in the Cloud, what is the procedure to access this data if it is known or suspected to reside outside your jurisdiction? Is international cooperation like the European Investigation Order or Mutual Legal Assistance Treaties the only route or do other options exist? Please elaborate.*

See above.

26. *What about data stored in the Cloud, where you are unable to determine the location of the server or the identity of the service provider?*

Most authors consider that access to the cloud pursuant to section 102/103, 110 (3) GCCP is permitted if the location of the service provider is unknown. The data secured from such clouds will most probably be considered admissible. If the identity of the service provider is unknown but the location is known to be outside Germany, access is considered illegal. For more information, see above.

27. *Can you legally access data in the Cloud, even if there is no app that links to this data or other direct link from the mobile device?*

If there is no direct link to the cloud, (direct) access through the mobile device pursuant to sections 102/103, 110 (3) GCCP is not permitted. If the cloud is on German servers, the authorities can request a search and/or seizure order by the local court and request cooperation from the provider.

28. *How is the access to data kept by a Service Provider related to the device regulated? Is it performed upon a Court order, or also through other means?*

Data storage by a provider of publicly accessible telecommunications services is regulated by the German Telecommunications Act. The GTA determines which data the providers can store and

can be shared with the authorities. In the GCCP you can find the corresponding provisions for requests to the provider. It is subject to intense scholarly debate whether providers of cloud services fall under the GTA (see Bruns, KK-StPO, 8 ed. 2019, § 100j, para. 3 with an overview over the debate).

All relevant requests (sections 100j GCCP, 102/103 GCCP, 94/95 GCCP) require a court order except in exigent circumstances.

29. *Does any of the foregoing depend on the type of crime involved (e.g. terrorism, child pornography etc.)?*

Open/transparent measures as described above generally apply to all type of criminal offenses. Searches and seizures could, however, be considered disproportionate for minor offenses. The type of crime is, however, very significant for secret measures as they refer to certain catalogues of crimes.

30. *Does not following the applicable rules always lead to inadmissibility of the evidence in this scenario? If not, please elaborate on exceptions and relevant conditions.*

No. In general, the German jurisprudence considers admissibility of evidence to be the rule. Only major, especially deliberate violations of procedural rules can lead to inadmissibility. The law defines certain exceptions for the protection of legal privilege and the core area of the private conduct of life (see above).

Please, answer all these questions separately for each scenario or instance which, in your opinion, is (partially) subject to different rules than other scenarios. At least, make the difference between the scenarios where a mobile device is seized and where it is not. If all sub-scenarios in one of these scenarios are the same, it suffices to only answer the questions once. However, most jurisdictions have different situations in which seizure is possible (e.g. in the context of a search of premises vs. not in the context of a search), so please differentiate between these scenarios, as well and answer the questions for them separately. If you prefer, you can answer the questions in their

formobile@netlaw.bg
Linkedin – Formobile-
Twitter – @Formobile2019
www.formobile-project.eu

totality in an integrated explanation, as long as all elements are covered and again, various scenarios are differentiated between.

Please, give as much guidance as possible to enhance our understanding. Always cite the provision of the law or the case law you are relying on (legal basis) and mention conditions, people involved in the action, formal requirements etc., even if not specifically asked.

Answer: Indication of length of answer: at least a couple of pages, as this is the main overview question.

31.* Question: In cases where the examination or data acquisition is not possible without changing the configuration of the device, is there a strict protocol that should be followed (e.g. procedure and changes should be tested, validated, and documented)? If yes, please specify on what rules this is based and what the requirements are. Please also provide examples.*

Answer: The GCCP does not contain any general provisions in this regard. The jurisprudence of the criminal courts and the German Constitutional Court have also abstained from establishing specific rules or procedures. The only provision addressing this issue is contained in section 100a (5), (6) GCCP and states:

"(5) In the case of measures under subsection (1) sentences 2 and 3, it must be ensured that technical means are in place so that

1. only the following can be intercepted and recorded:

a) ongoing telecommunications (subsection (1) sentence 2) or

b) the content and circumstances of the communication which could also have been intercepted and recorded from the date on which the order was made pursuant to section 100e (1) during ongoing transmission processes in the public telecommunications network (subsection (1) sentence 3);

formobile@netlaw.bg
Linkedin – Formobile-
Twitter – @Formobile2019
www.formobile-project.eu

2. only those changes are made to the information technology system which are essential in order to capture the data; and

3. the changes made are automatically reversed once the measure is concluded, insofar as this is technically possible.

The means used shall provide protection against unauthorised access using methods reflecting the state of the art. Copied data shall be protected against modification, unauthorised deletion and authorised inspection using methods reflecting the state of the art.

(6) A record is to be made of the following each time technical means are used:

1. the designation of the technical means and the time of their use,

2. information required to identify the information technology system and changes made which are not only transient,

3. information enabling the identification of the data captured and

4. the unit implementing the measure."

This provision is considered as "best practice" for other technical measures (Basar/Hiéramente, NStZ 2018, 681). It reflects the suggestions made by the Federal Office for Information Security that has published guiding principles for IT-forensics in 2011 (see https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Leitfaden_IT-Forensik.pdf;jsessionid=CB1575D92012E8267AD3DDE9974F77E4.1_cid502?__blob=publicationFile&v=2; see also Fährman MMR 2020, 228; Basar, FS Wessing, 2015, 635). These guiding principles have been referred to by a local court (AG Reutlingen, 5.12.2011 – 5 Gs 363/11) but are not legally binding (Fährman MMR 2020, 228). The guiding principles are 345 pages long.

formobile@netlaw.bg
Linkedin – Formobile-
Twitter – @Formobile2019
www.formobile-project.eu

***32.* Question:** *Are there any specific rules in criminal procedure that regulate the use of mobile forensics tools using/deploying AI technology? Are there any conditions which need to be met so AI-powered tools could be applied in the process of evidence collection?*

Answer: There are no specific rules in the GCCP that regulate forensic tools and/or AI technology. If such tools are used to review evidence already gathered through other (legal) means, it is possible that their use would be considered permissible as long as it does not replace any decision making by the relevant authorities.

***33.* Question:** *What are the main legal issues in your jurisdiction in the cases when mobile devices are involved in crimes across geographical boundaries? What procedures are foreseen to tackle these multijurisdictional issues? Should the forensic examiner be aware of the nature of the crime and the regional laws/legislative framework?*

Answer: The most debated issue in this regard is the access to data stored in a cloud (via mobile device or via a cooperation request to the provider). I am not aware of any procedures to tackle such issues. I believe it is absolute necessary that the forensic examiner be aware of the legislative framework. For more information, see above.

***34.* Question:** *Is there an established procedure/course of action to decide whether to apply the EIO or another instrument for cross-border gathering of evidence within the EU?*

Answer: As far as I am aware there is no established procedure/course of action established to determine when to rely on EIO or other instruments of cross-border gathering of evidence. The federal system leads to significant differences between the different States and/or prosecutors.

***35.* Question:** *Since, the abovementioned Directive does not preclude the application of MLAT by judicial authorities under some circumstances, what is the practice in your jurisdiction?*

Answer: I am not aware of a "practice" in my jurisdiction.

***36.* Question:** *Are you aware of any existing cooperation mechanisms and practices with the private sector?*

formobile@netlaw.bg
Linkedin – Formobile-
Twitter – @Formobile2019
www.formobile-project.eu

Answer: I am not aware of existing cooperation mechanisms with the private sector. It is known that some prosecutors have extensively relied on external IT-forensic experts to cope with the high demand for forensic expertise.

Section 2: Criminal procedure rules on analysis of data from mobile devices

***37.* Question:** *When data has been made accessible through mobile forensics, are there any rules on how the data must be analysed, especially to take into account:*

- *Data protection concerns (Law Enforcement Directive 2016/680 and implementing national law)*
- *Privacy concerns and respect for core area of private life (i.e. how is it guaranteed that very sensitive information, not relevant to the investigation is not used)*
- *Human rights such as the right to a fair trial (tools may deliver faulty results and methods used are often untransparent) and the right to non-discrimination (tools that are untransparent may contain bias)*
- *What information can be retained/copied? For how long?*

Please elaborate on both criminal procedure law, relevant data protection law and any other measures or guidelines that may exist. Please also cite and explain relevant case law.

Answer: Data protection concerns have to be taken into consideration. Section 500 (1) GCCP in conjunction with the **Federal Data Protection Act (sections 58 (2), 75 (2))** requires that information irrelevant for the proceedings is **deleted**. Information is irrelevant if it has no significance to the case (see also Basar/Hiéramente, NStZ 2018, 681). It may also be irrelevant if proceedings are terminated. In the first decision in this regard, the court decided that although the charges against the accused have been dropped pursuant to section 170 (2) GCCP, the information collected is still relevant until it is clear that the statute of limitations apply (BayObLG 27.01.2020 - 203 VAs 1846/19). The time limit therefore depends on the type of crime (see section 78 GCC).

formobile@netlaw.bg
Linkedin – Formobile-
Twitter – @Formobile2019
www.formobile-project.eu

Regarding **privacy concerns**, see above. The issue of human rights (fair trial and non-discrimination) have hardly been addressed by the courts.

formobile@netlaw.bg
Linkedin – Formobile-
Twitter – @Formobile2019
www.formobile-project.eu

Section 3: Admissibility of evidence before court

38. **Question:** *Are there general rules or guidelines on the admissibility of electronic evidence in your jurisdiction applicable to mobile forensics, not yet discussed above?*

Answer: See above.

39. **Question:** *Are the criteria for admissibility of evidence collected through mobile forensics the same as for the other types evidence? Please elaborate in any case.*

Answer: Generally speaking, the criteria for (in)admissibility of evidence are identical for all types of evidence. The only specific rules regarding types of evidence are those gathered through covert means (sections 100a and 100b GCCP).

40. **Question:** *What if procedural rules are not followed? Can evidence from mobile forensics still be submitted to the Court in certain circumstances, balancing out the interest of the criminal justice with the severity of the procedural breach?*

Answer: Such evidence can still be submitted. The general rule is that such evidence is admissible. The German courts adopt a balancing approach to determine a possible (exceptional) case of inadmissibility for severe procedural breaches.

41. **Question:** *Specifically, if data in the Cloud is accessed according to criminal procedure, but it turns out to be located outside your jurisdiction does this mean it is not admissible at all? Is it relevant that there was reasonable doubt about the location of the data at the time?*

Answer: There is no jurisprudence in this regard. The majority of scholars consider that **subsequent** knowledge about the location of the data outside Germany does not lead to its inadmissibility. The same probably holds true for **existing doubts prior to accessing the data**. Given the relatively strict jurisprudence regarding the inadmissibility of evidence in criminal proceedings, only a manifest violation of the rules (knowledge of data storage outside Germany) might lead to the inadmissibility of the evidence.

formobile@netlaw.bg
Linkedin – Formobile-
Twitter – @Formobile2019
www.formobile-project.eu

***42.* Question:** *What are the consequences if mobile evidence are altered either intentionally, or unintentionally due to their dynamic nature during the investigation process? Note that intentional alteration refers to using a process to uncover data which is known to alter some (meta)data, not to the falsification of evidence. The question is more whether any alteration, even on small and not relevant data may render the evidence inadmissible.*

Answer: Generally speaking, an alteration of evidence will not lead to its inadmissibility. Such **alterations** will be considered when **weighing the evidence** in a specific situation. The cornerstone of the GCCP in this regard is section 261 GCCP which stipulates:

"The court shall decide on the result of the taking of evidence at its discretion and conviction based on the entire content of the hearing."

It might also lead the judge to request an expert opinion (sections 72 et seq. GCCP).

***43.* Question:** *Specifically, are there rules on the used technology, methodology or standard, such as for example that this must be forensically sound as a prerequisite for admissibility? If yes, please elaborate.*

Answer: The GCCP contains no rule regarding the technology, methodology or standard as a prerequisite for admissibility.

***44.* Question:** *Are you aware of existing case-law in your jurisdiction, dealing with the admissibility of evidence produced using mobile forensics? If yes, please elaborate.*

Answer: I am not aware of any judicial decisions in this regard.

***45.* Question:** *Is there in your jurisdiction an established and recognised standardisation(s) of the processes of collection, analysis, interpretation and reporting of digital evidence that must be followed for the evidence to be admissible? (as critical to the validity of evidence, their quality and impact evidence's acceptance by the courts)? If yes, please elaborate.*

formobile@netlaw.bg
Linkedin – Formobile-
Twitter – @Formobile2019
www.formobile-project.eu

Answer: I am not aware of any established and recognised standardisation that is relevant for the admissibility of evidence. For the guiding principles see above.

46. **Question:** *Is a failure to comply with Data Protection law, or privacy rules in itself, enough to refuse admissibility of the evidence, even when procedure is otherwise followed?*

Answer: Data protection law only applies insofar as the GCCP does not contain more specific provisions (section 500 (1) no. 1 GCCP) making it unlikely that a violation of Data protection law occurs if the procedures established in the GCCP are followed. There is no specific provision or jurisprudence regarding the issue of inadmissibility as a result of data protection law violations. I consider it highly unlikely that German courts would consider evidence in a criminal case as inadmissible for (mere) violations of data protection law.

47. **Question:** *Is there case law in your jurisdiction on evidence collected through mobile forensics having been questioned or rejected in Court because the admissibility was questioned? If yes, please elaborate on at least 3 cases.*

Answer: I am not aware of such case law.

formobile@netlaw.bg
Linkedin – Formobile-
Twitter – @Formobile2019
www.formobile-project.eu

Section 4: Interpretation and presentation of evidence from mobile forensics before the Court

48. **Question:** *Are there general rules or guidelines on the interpretation and presentation of evidence from mobile forensics, such as:*

- *Is mobile forensic evidence given a certain probative value?*
- *Are there rules on how to interpret mobile forensic evidence or requirements which must be complied with for the evidence to be considered reliable?*
- *Must such evidence be examined by an expert witness?*
- *If not obligatory, is this a common practice?*
- *What are the requirements for experts (experience, independence, training, etc.)?*
- *Is there a centralised management of mobile forensic operations in your jurisdiction to ensure the work is compliant with standards and can be presented in court in a consistent manner?*

Answer: Mobile forensic evidence is not given a certain probative value. However, judges tend to rely heavily on such evidence in practice. The GCCP does not contain any rules on how to interpret mobile forensic evidence and does not define any specific requirements. I am also not aware of any other binding rules and requirements in this regard. Such evidence must not be examined by an expert witness (see section 261 GCCP cited above). However, it is common practice to request testimony from expert witnesses - mostly from the Landeskriminalamt (state criminal police) – to further explain the (meta) data. Experts should have experience in the field. However, the GCCP grants some leeway to the judge to select an expert. Section 73 GCCP states:

(1) The judge shall select the experts to be consulted and shall determine their number. He shall agree with them on a time limit within which their opinions may be rendered.

(2) If experts are publicly appointed for certain kinds of opinions, other persons are to be selected only if this is required by special circumstances.

formobile@netlaw.bg
Linkedin – Formobile-
Twitter – @Formobile2019
www.formobile-project.eu

There is no explicit provision that determines the degree of independence of an expert (contrary e.g. to the provision regarding the independence of experts for DNA-investigations, see section 81f (2) GCCP). Other participants may challenge the expert if its independence is in doubt (section 74 GCCP).

There is cooperation between police authorities in ZAC ("Zentrale Ansprechstelle Cybercrime") in order to strengthen the capabilities in this regard.

49. **Question:** *Are you aware of existing case-law in your jurisdiction dealing with the interpretation and presentation of evidence produced using mobile forensics? If yes, please elaborate.*

Answer: I am not aware of such case-law.

50. **Question:** *Is there in your jurisdiction an established and recognised standardisation(s) of the processes of collection, analysis, interpretation and reporting of digital evidence that must be followed for the interpretation and presentation of evidence before a court? Or alternatively which is not obligatory but considered as critical for the validity of evidence, its quality or the impact of the evidence and its acceptance by the courts? If yes, please elaborate.*

Answer: There is no established and recognised standardisation that is binding. For the guiding principles on IT-forensics, see above.

51. **Question:** *Is there case law in your jurisdiction on evidence collected through mobile forensics having been questioned or rejected in Court because of interpretation issues or presentation issues (e.g. considered admissible but not reliable)? If yes, please elaborate on at least 3 cases.*

Answer: I am not aware of such case law.

formobile@netlaw.bg
Linkedin – Formobile-
Twitter – @Formobile2019
www.formobile-project.eu

Section 5: Implications of the use of mobiles forensics on the role of the different parties in the trial

52. **Question:** *Are there rules or guidance, or is there case law in your jurisdiction on how to respect the right to a fair trial in case of evidence extracted via mobile forensics? What practices are established in view of the respect of the principle of equality of arms?*

Answer: There are **no clear rules in the GCCP** in this regard and no common practices. The Federal Court of Justice has hinted at the necessity to provide access to forensic software to the accused in a case where, as a consequence of the forensic work of the police, the accused was not able to access the relevant data with normal means because of a change of format (BGH, BGH, 11.2.2014 – 1 StR 355/13). Other courts have granted additional funding to court appointed lawyers for the extra costs of storage of masses of data (OLG Hamm, 6.5.2015, 2 Ws 40/15). These decisions only pertain to the question of costs. Some courts also decided that the right to a fair trial requires the defense to receive a digital copy of data gathered in the proceedings (see e.g. LG Regensburg, 24.7.2017 – 6 Ws 29/17). Other courts have objected and, inter alia, referred to the data protection rules.

53. **Question:** *Is there any training required by law for the judges, prosecution, expert witnesses, lawyers involved in cases with evidence coming from mobile forensics?*

Answer: I am not aware of any specific training requirements for judges and prosecution as well as lawyers. Expert witnesses do not require specific trainings but need to qualify as experts which normally requires a certain track record in the field.

54. **Question:** *Is there a pre-determined time duration/limitation period required for the extraction of evidence from mobile devices, time for decoding, reviewing and analysing of the data, time for reporting that data in a form that prosecutors and others can use?*

Answer: There is no pre-determined time duration or limitation period. The German Constitutional Court explicitly stated that the review process envisaged in section 110 GCCP is not bound by any

formobile@netlaw.bg
Linkedin – Formobile-
Twitter – @Formobile2019
www.formobile-project.eu

specific time limits (BVerfG, 30.1.2002 - 2 BvR 2248/00). The review process must be done in an appropriate time (BVerfG, 29.1.2002 - 2 BvR 94/01).

***55.* Question**: *What are the procedural rights inherent to the different participants in a criminal procedure (i.e. the prosecution, the court, the defendant, the witness, the victim, etc.)?*

Answer: I do not fully understand this question. Please let me know what procedural rights you are interested in,

5.1 The Prosecution

***56.* Question:** *Are there any requirements or guidance provided to the prosecution as how to control and deal with mobile forensics and evidences?*

Answer: I am not aware of any such requirements or guidance.

5.2 The Court

***57.* Question:** *Is there judicial control over the approaches and methods used for acquiring, collecting and analyzing evidence? Please refer to case law if possible.*

Answer: Generally speaking, there is no judicial oversight over the analysis of data collected in a legal way (for details see above). If there is an indication that the analysis violates right of the accused, the accused may request a ruling by the Court pursuant to an analogous application of section 98 (2) s. 2 GCCP. There is a possibility of appeal to the Regional Court.

***58.* Question:** *How does the Court assess the evidence obtained via mobile forensics? Please refer to case law if possible to illustrate the approach.*

Answer: There are no specific rules or processes regarding the assessment of the evidence. The Court is only bound by section 261 GCCP which grants a significant leeway to judges.

formobile@netlaw.bg
Linkedin – Formobile-
Twitter – @Formobile2019
www.formobile-project.eu

5.3 The defendant and defender

59. **Question:** *Are there rules and standards regulating the defendant and his/her defender's rights to access and to make copies of the acquired mobile evidence? Are they able to get any information on the process used to acquire mobile forensic evidence (e.g. information on how the tools work, the procedures used, the parties involved and how the validity of the results is guaranteed)? Please refer to case law if possible.*

Answer: There is a right by the defence counsel to review the evidence, to take notes and to make copies necessary for the defence. It is subject to debate whether this right entails a right to make/receive a **copy of the mobile forensic evidence**. Some courts and the majority of authors consider that the defence should receive such a copy in order to review the documents in his/her offices and with the accused (see e.g. LG Regensburg, 24.7.2017 – 6 Ws 29/17 with further references; Meyer-Goßner/Schmitt, 62. ed. 2019, § 147, para. 19c; El-Ghazi, jurisPR-StrafR 21/2017; Basar jurisPR-StrafR, 14/2016 Anm. 1). Others still consider such copies as "evidence" which – for traditional reasons and to protect the integrity of the evidence – could only be accessed on the premises of the police, prosecution or court.

Normally, the case files contain an extraction report that details the program and methods used by the forensics department of the Landeskriminalamt. It describes date and time as well as the relevant tools. The case files rarely contain additional information in this regard.

5.4 Witnesses

60. **Question:** *During the pre-trial stage, how is the right to privacy of the witnesses preserved? Are there any practical steps taken to exclude certain types of information which are cumulatively non-relevant to the case and too private? Are there particular requirements for witnesses regarding their capability to testify in terms of mobile forensics both in the pre-trial and the trial phase of the criminal proceedings? Please refer to case law if possible.*

Answer: The case file has to be complete and the defence counsel is normally granted unlimited access to the case files as well as the evidence. There are some discussions as to whether the defence counsel can receive a digital copy of the evidence (see above). In the pre-trial stage, the prosecution can reduce access to the case file pursuant to section 147 (2) GCCP which states:

"If the fact that the investigations have been concluded has not yet been recorded in the file, defence counsel may be refused inspection of the files or of individual parts of the files as well as the viewing of items of evidence in official custody insofar as this may jeopardise the purpose of the investigation."

If information is not relevant for the case, the witness can request its **deletion** pursuant to section 500 (1) GCCP in conjunction with section 58 (2) Federal Data Protection Act. If the information is relevant and sensitive, it will be accessible to the defense.

There are no particular requirements for witnesses regarding their testimony.

5.5 The Victim

61. **Question:** *How are the victim's/victims' rights ensured during both the pre-trial and the trial phase of the proceedings? How is their privacy preserved? Can they use the evidence obtained via mobile forensics when exercising their rights? Please refer to case law if possible.*

Answer:

There is no specific provision as to the rights of the victim in the proceedings. The privacy of the victim is preserved by virtue of section 32f (5) GCCP which states:

"Persons who are granted inspection of the files may, neither in full nor in part, publicly disseminate those files, documents, hard copies or copies which were surrendered to them pursuant to subsection (1) or (2), nor may they be transmitted or made available to third parties for purposes other than the proceedings in question. They may use personal data which they have acquired in accordance with subsection (1) or (2) only for the purpose for which they were granted inspection

formobile@netlaw.bg
Linkedin – Formobile-
Twitter – @Formobile2019
www.formobile-project.eu

of the files. They may use these data for other purposes only if they could be permitted information about them or inspection of the files for those purposes. Persons who are granted inspection of the files are to be made aware of the limitations as to use.

Under certain circumstances, the public can be excluded from part of the trial to protect the victim (see sections 171b, 172 Courts Constitution Act). The victim has also a right to access the case files pursuant to section 406e GCCP and may use the information in private proceedings against the accused.

formobile@netlaw.bg
Linkedin – Formobile-
Twitter – @Formobile2019
www.formobile-project.eu

Section 6: Comments

If you feel some important elements of your national law relating to the use of mobile forensics in criminal investigations have not sufficiently been covered, please explain them here. If you feel an overview is missing, please also provide guidance on this below.

Answer: Indication of length of answer: few paragraphs up to a couple of pages.