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

DENMARK:

Report issued by Jørn Vestergaard, Professor Em. of Criminal Law

Introductory questions:

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

Answer: Indication of length of answer: one line.

University of Copenhagen, Faculty of Law, Professor Em. of Criminal Law

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

Answer: Indication of length of answer: one line.

University of Copenhagen

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: Indication of length of answer: couple of lines.

In the Administration of Justice Act/ the Procedural Code (retsplejeloven), varying terms are utilized in the chapters regulating the use of forensic measures.[1]

In relation to acquisition from Service Providers of teledata in criminal cases, the term "telephones or other similar communication devices" is used as a common denominator for

[1] A consolidated online version of the Act can be read here: https://pro.karnovgroup.dk/document/7000840230/1?frt=consolidated&hide_flash=1&page=1&rank=6

See also Langsted, L.B. et al: *Criminal Law in Denmark*, Fifth Edition, Wolters Kluwer 2019.

devises that communicate via telecommunication, e.g. cellphones, tablets and smartwatches. Furthermore, the term "gps eller et andet tilsvarende apparat" [gps or another similar device] is used, see examples below.

The Procedural Code regulates wire-tapping by use of the term "aflytte telefonsamtaler eller anden tilsvarende telekommunikation" [interception of telephone-conversation or other similar telecommunication], cf. § 780(1)(1). The term "anden tilsvarende telekommunikation" even covers incoming e-mail.

The Procedural Code even regulates police monitoring of telecommunication between "telefoner eller andre tilsvarende kommunikationsapparater" [telephones or other similar communication devices], cf. § 780(1)(3 and 4) and § 786 regarding "teleoplysning" [teleinformation].

Further, the Procedural Code regulates teleobservation by use of the terms "mobiltelefon" [mobile phone], cf. § 791(a)(5)(1) and "gps eller et andet tilsvarende apparat" [gps or annother similar device), cf. § 791(a)(5)(2).

Finally, the Procedural Code regulates data electronic extraction from "et informationssystem" [an information system], including smart phones, cf. § 791(b) regarding "dataaflæsning".

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:*

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

Mobile device not seized

4. *Under what circumstances can a mobile device be read or searched without seizing it?*

Telephone tapping requires a court order, except if the matter is urgent (*periculum in mora*). The main conditions are (1) that there is probable cause to suspect communication to or from a suspect, (2) that such inception is important for the investigation, and (3) that (a) the offence is punishable by imprisonment for 6 years or more, (b) involves a crime against the state or terrorism, or (c) involves specific offences listed in the law, cf. § 781(1-3).

A court order concerning electronically reading or "searching" (dataaflæsning) a mobile device [a communications-system] without seizing it requires probable cause to suspect that it is used by a suspect in relation to a planned or committed offence punishable by imprisonment for 6 years or more (or a terrorist offence or a state crime). A court order is required, except if the matter is urgent (*periculum in mora*). The measure must not be disproportionate in relation to the intrusion and inconvenience for the suspect. Cf. § 791(b).

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?*

With regard to telephone tapping, the principle of proportionality must be respected, cf. § 782(1). If the investigation concerns crimes against the state, terrorism, or other particularly serious offences, the court can allow that not only a specific telephone is intercepted, but that all devices used by the suspect are tapped, cf. § 783(2). Telephone tapping is prohibited with regard to communication between a suspect and a priest, a lawyer, a physician, etc., cf. § 782(2). If the matter is urgent and the measure has been initiated by the police without a court order, the court must immediately and within 24 hours be informed in order for the court either to approve the measure or to issue a proper court order. If the court finds that the measure should not have been enacted, the Ministry of Justice must be informed, cf. § 783(4).

With regard to reading a mobile device (dataaflæsning), conditions equivalent to those regulating ordinary search applies, cf. § 791(b)(3 and 4). The court order must stipulate a timeframe for the search. The period must be as short as possible and not exceed 4 weeks. The court may extend the timeframe by maximum 4 weeks at the time. Reading messages in real time requires that the general requirements regarding wire-tapping be met. Conditions equivalent to those regulating wire-tapping applies, see answer above.

6. *Is it allowed to use technical tools to bypass security?*

Yes, depending on the above mentioned legal requirements, e.g. by installation of a sniffer program (dataaflæsning).

7. *Can information be copied or only read at this stage?*

Normally, investigation is conducted on a copy of the materials.

8. *Is consent of the owner/person in possession of the mobile device necessary?*

No, provided that the above mentioned legal requirements are met.

9. *Can the owner/person in possession of the mobile device be forced to unlock the device?*

The Supreme Court has approved that the police may force a suspect to unlock a smartphone by pressing the suspect's thumb on the phone's fingerprint-reader, provided that the general requirements for search of a device are met. If retrieving the data is urgent, no prior court order is required (*periculum in mora*). The judgement is published in Ugeskrift for Retsvæsen, U 2019.1304 H.

10. *Must the owner/person in possession of the mobile device be informed?*

The main rule is that the individual subject to a secret measure must subsequently be notified about the measure. Cf. § 788 ad telephone-interception, etc., and § 791(b)(4) ad reading of content (dataaflæsning). On request by the police, the court may on certain conditions permit omitting or postponing such notification.

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

11. *Who can order a search and what are the formal requirements, if any?*

A suspect's objects can be searched if there is reasonable cause for suspicion regarding a criminal offence punishable by imprisonment, cf. § 794. The police is in any case authorised to perform a search of an unlocked object. If the device is locked, a court order is required, unless it is urgent to conduct the search, cf. § 796(2-3). A court order is not necessary if the owner of the device consents in writing, cf. § 796(5).

A search of a device/an object belonging to a non-suspect can be conducted if the case concerns an offence punishable by imprisonment, and there is probable cause to suspect that evidence or objects relevant to the case may be found. A court order is required, unless it is urgent to conduct the search. Cf. § 795 ff. A court order is not necessary if the owner of the device consents in writing, cf. § 795(1).

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

See answer to Q 11.

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.*

The Supreme Court has approved that data stored on a server located outside Danish jurisdiction may be retrieved without involving foreign authorities, provided that the general requirements with regard to the measure are fulfilled, and that the relevant login information is available. The judgement has been published in Ugeskrift for Retsvæsen, U 2012.2614 H.

The National Procecutor (Rigsadvokaten) has issued guidelines regarding acquisision of electronic evidence from international Service Providers (Rigsadvokatens meddelelse om indhentelse af elektroniske oplysninger fra internationale serviceudbydere). See also The National Prosecutor's

guidelines regarding international legal assistance (Rigsadvokatens meddelelse om International Retshjælp).

Due to the general Danish reservation regarding JHA, Denmark is not party to the EIO.

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

The provisions regarding terrorist offences and state offences (Penal Code Chapts. 12 and 13) and the statute regarding child pornography (Penal Code § 235) is included in the list of offences establishing a basis for wiretapping/bugging/interception, etc., regardless of the general requirement concerning sentencing latitude (i.e. imprisonment for 6 years or more). An additional list of offences is included, too. Cf. § 781(1)(3). Similar rules regulate the authorization of teleobservation regarding the localization of a device, cf. § 791(a)(5).

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.*

In general, illegally obtained evidence will be admissible in court. Danish law does not have particular exclusionary rules. No doctrine addressing 'the fruits of the poisoned tree' applies. Thus, the court's mode of assessing the evidence is not constrained or regulated by specific rules. The legal tradition cherish the principle of the material truth, and judicial practice regarding admission of illegally obtained evidence is very liberal and permissive, the presumption being that available evidence shall normally not be excluded. The assessment of evidence is 'free' for the court to make, cf. § 880.

If a piece of evidence that have not and could not have been produced legally has been obtained by coincidence in line of an otherwise legal interception or search, the police always may use the available information for investigating the offence in relation to which the measure was legally implemented. But, as a main rule, such derivative information may not be presented in court in relation to another offence, if the actual measure could not legally have been employed in relation

to that offence. However, the court may discretionarily admit such information under the following cumulative conditions: (1) if other types of investigative measures are not suited to secure adequate evidence, (2) if the suspected offence is punishable by imprisonment for up to 1 year and 6 months, and (3) the court finds admission necessary. Cf. § 789(1-3) ad interception, and § 800(1-2) ad search. In accordance with recent amendments to the two cited provisions such evidence is always admissible in cases concerning disbandment of an unlawful association (= a criminal gang), cf. § 789(4) and § 800(3).

In case of violation of procedural requirements, the Ministry of Justice shall be notified, cf. § 783(2 and 4 in fine) regarding wiretapping, etc.

Mobile device seized

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

A suspect's objects may be seized if there is reasonable cause for suspicion regarding a criminal offence, and there is reason to believe that the object is relevant as evidence, or should be confiscated, or should be returned to the proper owner. In principle, a decision regarding seizure must be issued by the court, except if it is urgent that the police executes the measure, or a written consent is issued by the owner. Cf. §§ 801 ff. (§ 802 ad suspects/§ 803 ad non-suspects). A court order is not necessary if the owner of the device consents in writing. Cf. § 806(9).

With regard to acquisition from Service Providers of information concerning connections between telephones or other electronic devices, the rules regarding wiretapping/ bugging/ interception applies, cf. § 801(3) and § 780(1)(3).

If a device has been seized and the content can be read without the assistance of a Service Provider, the device may be searched in accordance with the general rules on searches, cf. the statuary conditions referred ad Q 11. See also High Court decision published in Ugeskrift for Retsvæsen, U 2008.1734 V.

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

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

See answer to Q 16.

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

The general requirements regarding a search must be adhered to. See answer to Q 11.

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?*

The general principle of proportionality is stated in all relevant provisions in the Procedural Code, including in the chapter regarding the requirements for conducting a search, cf. § 797. The principle of parsimony is explicitly stated with regard to the implementation of a search, cf. § 798(1). See also correspondent's answer to Q 37.

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

A court order is not necessary if the owner of the device consents in writing. Cf. § 795(1) (non-suspects) and § 796(5) (suspects).

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

Yes. See answer to Q 9.

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

Yes, the same rules as mentioned under Q 10 apply. Cf. § 799(2).

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

Yes, depending on the general legal requirements.

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

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

The relevant technical tools may be used in all cases.

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 answer to Q 13.

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?*

See answer to Q 13.

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?*

Yes, se answer to Q 13.

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?*

Providers of telecommunication services are obliged to assist the police in intercepting teleinformation, etc., cf. § 786(1) and Ministerial Order, bkg. 1145, 2006.

Service Providers are obliged to log telecommunication (except internet communication) for at least 1 year, cf. § 786(4) and Ministerial Order, bkg. 988, 2006 as revised by bkg. 660, 2014, and Ministerial Guidelines, vejl. 74, 2006.

The police may order a Service Provider to urgently secure electronic data, including regarding tele-traffic, and to immediately provide the police with teledata regarding other Service Providers relevant to the case. Cf. § 786(a).

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

A Service Provider is obliged to deliver information regarding call history from a stolen cellphone, if the proper owner consents, see judgement made by the High Court, reported in Ugeskrift for Retsvæsen, U 1996.169 Ø.

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

The general requirement is that the offence is punishable by imprisonment for 6 years or more. Further, an additional list of offences qualify, including child pornography, terrorist offences and state offences. See answer to § 14.

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. See answer to Q 15.

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 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.

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

***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: Indication of length of answer: 1-2 paragraphs.

When securing data on an electronic device, standard procedures are complied with, whether or not the configuration needs to be altered. The proper procedure is defined in detail. The tools applied for acquisition and line of action must be documented. Method and procedure is prescribed on the basis of internal quality specifications with a view to valid and sustainable provision of evidence in legal procedings. Securing data is exclusively the responsibility of specially trained staff. In order not to compromise data on the device, analysis of content is conducted on a duplicate of the materials, not directly on the device.

(Source: Information kindly provided by senior officer at the National Center for Cyber Security, NC3)

***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: Indication of length of answer: 1-2 paragraphs.

No specific rules have been stipulated. If AI technology is applied, conclusions are not drawn entirely on the basis of results produced by one single tool. Dual tool verification is utilized in order to validate conclusions. In addition, results are always examined manually, e.g. when comparing data.

(Source: Information kindly provided by senior officer at the National Center for Cyber Security, NC3)

***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: Indication of length of answer: couple of paragraphs

Depending on domestic legislation and legal traditions in other countries, transnational police investigation is notoriously characterized by vast bureaucracy. In particular, is can be cumbersome to work on the basis of MLAT. Often requests are not answered expediently or within a reasonable timeframe. Normally, cooperation within Europol and Interpol is functioning more smoothly. Sienna is an ideal example of fairly swift and flexible cooperation. Every staff member under the National Police Commisioner (Rigspolitiet) working with it-criminality is familiar with possibilities and challenges regarding international police cooperation. Any contact to foreign law enforcement entities is communicated through official channels.

(Source: Information kindly provided by senior officer at the National Center for Cyber Security, NC3)

***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: Indication of length of answer: 1-2 paragraphs.

Due to the general Danish reservation regarding JHA, Denmark is not party to the EIO. Evidence is retrieved via Europol and Interpol.

***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: Indication of length of answer: 1-2 paragraphs.

See answer to Q 33 and Q 34.

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

Answer: Indication of length of answer: 1-2 paragraphs.

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

The National Cyber Crime Center's public-private-partnerships operate exclusively within the realm of crime prevention, e.g. targeting sexual offences, stalking, hacking, attacks on it-systems, economical crime.

(Source: Information kindly provided by senior officer at the National Center for Cyber Security, NC3)

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

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: Indication of length of answer: couple of paragraphs.

When analyzing extracted data, various verified and authorized tools are utilized. The tools are applied by specially trained and certified staff. Technical reports are based on a standard template. Staff members often give testimony as expert witnesses in court proceedings.

Data protection practice must be in compliance with the GDPR. The National Police Commissioner operates a Centre for Data Protection (CfD) assigned to administer and monitor all other units.

Only relevant data are looked into, so that the acquisition of data is not going to be more invasive than necessary. As a main rule, the local police district issues a statement regarding topics of interest for the investigation, and the analyst uses this information as a point of departure.

Data of no relevance for the investigation will not be looked into, which in principle means that private and/or confidential information is not included in the investigation. Provisions in the

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

Procedural Code covering matters regarding right of exemption from the duty to give evidence are respected. In case of controversy, the issue may be brought up in court.

Results from the analysis are documented and validated in order to secure that they can be presented in court and be interpreted by a police expert wittness.

Data and analysis results are archived in accordance with statutory and administrative provisions.

(Source: Information kindly provided by senior officer at the National Center for Cyber Security, NC3)

Correspondent's note:

If the owner of a device maintains that it contains private/sensitive information, a court order may instruct the police to weed out such information. In a recent case involving a weekly magazine, the police was ordered to involve external expertice in order to to assist the prosecutor and the publishing company in reviewing seized materials and sponge out items covered by journalistic confidentiality. See Supreme Court judgement published in Ugeskrift for Retsvæsen, U 2015.1249 H. A media person (physical or legal) may demand that the first review is conducted by the court, cf. § 807(3).

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: Indication of length of answer: 1-2 paragraphs.

See answer to Q 15.

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: Indication of length of answer: 1-2 paragraphs.

There are no particular rules regarding the admissibility of evidence collected through mobile forensics. See even answer to Q 15.

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: Indication of length of answer: 1-2 paragraphs.

Under Danish procedural law, the court's evaluation of evidence presented is not bound by formal rules of any kind. In accordance with legal tradition, certainty beyond reasonable doubt is required for a guilty verdict (*in dubio pro reo*). See even answer to Q 15.

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: Indication of length of answer: 1-2 paragraphs.

No! See answers to Q 13 and Q 15.

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: Indication of length of answer: couple of paragraphs.

In order not to compromise data on the device, analysis of content is conducted on a copy of the materials, not directly on the device. See even answer to Q 31.

As previously mentioned, the court's evaluation of evidence presented is not bound by formal rules under Danish procedural law. See even answer to Q 15 and Q 40.

***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: Indication of length of answer: 1-2 paragraphs.

No particular rules to that effect exist with regard to 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: Indication of length of answer: 1-2 paragraphs.

No such case-law has been published.

***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: Indication of length of answer: 1-2 paragraphs.

No standardized processes have formally been established by statute or court practice. However, the National Cyber Crime Center, NC3, has defines specific standards, see answer to Q 31.

***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: Indication of length of answer: 1-2 paragraphs.

No. See answer to Q 15.

***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: Indication of length of answer: 3+ paragraphs.

No such case law has been published.

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: Indication of length of answer: couple of paragraphs.

The National Attorney General (Rigsadvokaten) and the National Police Commissioner (Rigspolitichefen) have jointly issued guidelines regarding special attention points in the use of teledata and mobile data in criminal cases (Anvendelse af teledata i straffesager, rev. 22.06.2020): https://vidensbasen.anklagemyndigheden.dk/h/6dfa19d8-18cc-47d6-b4c4-3bd07bc15ec0/VB/f3046eca-c8fb-449a-9074-b8ecccf45a16?showExact=true

Depending on the merits of the case and the information presented to the court, an expert witness sometimes appears i court, typically an experienced specially trained police officer.

As previously mentioned, the National Police Commissioner (Rigspolitiet) operates a highly specialized unit, the National Cyber Crime Center, NC3. See answers to Q 31 ff.

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

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: Indication of length of answer: 1-2 paragraphs.

No such case law has been published.

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: Indication of length of answer: 1-2 paragraphs.

See answer to Q 31 ff.

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: Indication of length of answer: 3+ paragraphs.

No such case law has been published.

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: Indication of length of answer: couple of paragraphs.

As prviously mentioned, the National Attorney General (Rigsadvokaten) and the National Police Commissioner (Rigspolitichefen) have jointly issued guidelines regarding special attention points in the use of teledata and mobile data in criminal cases (Anvendelse af teledata i straffesager, rev. 22.06.2020):

https://vidensbasen.anklagemyndigheden.dk/h/6dfa19d8-18cc-47d6-b4c4-3bd07bc15ec0/VB/f3046eca-c8fb-449a-9074-b8ecccf45a16?showExact=true

Prosecutors, defense attorneys and judges have been informed of said guidelines.

No relevant case law has been published.

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: Indication of length of answer: couple of paragraphs.

No such training is currently taking place on a regular/systematic basis. However, expert witnesses have special training, se answer to Q 37 and Q 48.

The Minister of Justice has announced, that comprehensive training programs concerning the use of digital forensics and evidence will be introduced. Advis to Parliament's Judiciary Committee in the Spring of 2020 (Orientering om status for implementering af tiltag i teledata-sagen, Justitsministeriet 30 April 2020).

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

***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: Indication of length of answer: 1-2 paragraphs.

No, not to my knowledge.

***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: Indication of length of answer: couple of paragraphs per different participant.

Prosecution: Under Danish law, the public prosecution service is distinct from the judiciary. The national prosecution service is hierarchic and is headed by the non-political Attorney General (Rigsadvokaten). At the intermediate level, two regional District Attorneys (de regionale statsadvokater) and a specialized unit regarding economic and international crime, operates. At the local level, the chief constable of police is head of the prosecution service. The decision regarding whether or not to prosecute rests with the prosecution service. Decisions to indict are governed by a principle of objectivity, cf. § 96. Still, there is some leeway for semi-discretionary non-prosecution/waiver of prosecution, cf. § 722. Private prosecution is reserved for certain cases regarding libel or intrusion in privacy. Preparing for trial, the prosecutor must submit a list of evidence, cf. § 837. At trial, the prosecutor presents an opening statement and commence the questioning of the defendant. In the following, the trial mode is adversary.

Judiciary: A criminal case will be dealt with by one of the municipal courts and may be appealed to one of the two regional High Courts by either the defendant or the prosecutor. In more serious cases, lay assessors join the court, and in the most serious cases, jurors join the court.

Defendant: In more serious cases, a defense attorney must be appointed, presumptively principle in accordance with the defendant's preference. In principle, the defendant and the defender must be present in court. The attorney has access to all relevant materials.

Regarding witnesses' and victims' rights, see answers to Q 60 and Q 61 below.

For further details, see Langsted, L.B. et al: *Criminal Law in Denmark*, 2019.

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: Indication of length of answer: couple of paragraphs.

The National Attorney General (Rigsadvokaten) and the National Police Commissioner (Rigspolitichefen) have jointly issued guidelines regarding special attention points in the use of teledata and mobile data in criminal cases (Anvendelse af teledata i straffesager, rev. 22.06.2020): https://vidensbasen.anklagemyndigheden.dk/h/6dfa19d8-18cc-47d6-b4c4-3bd07bc15ec0/VB/f3046eca-c8fb-449a-9074-b8ecccf45a16?showExact=true

The guidelines and appended instructions have been issued in the wake of a comprehensive technical analysis conducted by Deloitte in order to locate the various types of errors and flaws resulting from conversion of teledata from Service Providers.

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: Indication of length of answer: couple of paragraphs.

It is basically the task of the defense attorney to challenge evidence after consultation with the client.

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

In cases regarding teledata, a specially trained police officer or other it-specialist might appear before the court as expert witness, see answer to Q 48.

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: Indication of length of answer: couple of paragraphs.

The assessment of evidence is free, see answer to Q 15.

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: Indication of length of answer: couple of paragraphs.

In general, a defense attorney has access to all evidence material and typically receives copies, cf. § 792(a)(3). Normally, the defense attorney does not know how data retrieved from a mobile device has been extracted and analyzed. Focus will typically be on the available data, and the defense will be established in accordance with the client's reactions to the information presented. According to an experienced defense attorney, the validity of evidence based on mobile forensics is seldom an issue.

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*

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

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: Indication of length of answer: couple of paragraphs.

During investigation, the police cannot force an individual to submit oral evidence, cf. § 750.

Interception is prohibited with regard to a suspect's communication with a priest, a lawyer, a physician, etc., cf. § 782(2). Materials produced in violation of this must immediately be destroyed, unless it indicated that an offence has been committed by the witness, cf. § 791(3). Similar rules apply in relation to search and seizure of objects belonging to such a witness or a member of the press, cf. § 794(3) and § 795(2) ad search, and § 802(4) ad seizure.

An individual exempted from the duty to appear as a witness in court due to family relations, etc., is not in that capacity protected by the modifications regarding search and seizure. See also answers to Q 15 and Q 37.

Regarding expert witnesses, se answer to Q 37 and 48.

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: Indication of length of answer: couple of paragraphs.

The victim of a serious violent or sexual offence has the right to have an attorney assigned (bistandsadvokat), cf. §§ 741(a) ff. The attorney has access to relevant materials and is entitled to object to the use of evidence in violence of the victim's privacy, e.g. prior sexual experience.

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.

- As the questionnaire is concerned with mobile forensics in particular, the correspondent has not elaborated on issues regarding the retrieving of telecommunication data from Service Providers and other types of digital forensics. However, it might be noticed that a major teledata scandal and a number of other problems has haunted the Danish criminal justice system since the beginning of 2019. An overview of topics was presented to Parliament's Judiciary Committee in the Spring of 2020 (Orientering om status for implementering af tiltag i teledata-sagen, Justitsministeriet 30 April 2020).

- In the Spring of 2019 it became publicly known that conversion of data retrieved from Service Providers had been severely flawed. A massive effort in order to mend the problems has been implemented, and a comprehensive review of more than 10.000 cases is conducted under the supervision of an independent control- and steering group. See various accounts in English here:

https://www.europarl.europa.eu/doceo/document/E-9-2019-002673_EN.html

https://www.europarl.europa.eu/doceo/document/E-9-2019-002673-ASW_EN.html

https://www.theguardian.com/world/2019/sep/12/denmark-frees-32-inmates-over-flawed-geolocation-revelations

https://edri.org/danish-data-retention-back-to-normal-after-major-crisis/

- In the Spring of 2020, a supplier of software to extract and analyze data from iOS devices informed the National Police Commissioner (Rigspolitiet) that errors had been discovered in two software tools, e.g. iPhones. One tool is used in mobile forensics by the National Cyber Crime Center, NC3, the other by the local police districts. The errors concern the time stamping of certain

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

digital data, ie. metadata regarding the date for formation, reading, or editing, of a file, e.g. a picture. After reviewing all relevant cases, it is the conclusion of the National Police Commissioner (Rigspolitiet) and the Attorney General (Rigsadvokaten) that the errors have not flawed evidence significantly in any criminal case. The supplier has now amended the software. See information to Parliament's Judiciary Committee (Orientering om politikredsenes gennemgang af sager efter fejl i softwareværktøj, Justitsministeriet 11 June 2020.)

- Further, it was discovered that data delivered from Service Providers in the course of telephone interception were incomplete and flawed. Se information to Parliament's Judiciary Committee (Foreløbig orientering om ufuldstændige mobildata i forbindelse med telefonaflytninger, Justitsministeriet 5 May 2020).

- In order to address the problems mentioned above and certain other current problems, the National Police Commissioner has initiated an external comprehensive thematic review of applied digital forensics with a view to establish standardized methods and procedures for declaration and validation and for training of specialists in digital forensics. More than 400 it-systems operated by the police and the prosecution are under scrutiny by external specialists.

- The Minister of Justice is preparing the creation of an independent supervising agency concerning the use of all technological forensics and evidence. The agency shall ensure that the uncertainty regarding the validity of specific data are disclosed fully throughout the whole chain of criminal procedure. On 21 February 2020 a draft bill was presented to Parliament's Judiciary Committee (Retsudvalget 2019-2020, bilag 373). Due to covid-19, the legislative process has been delayed.

Copenhagen 14 August 2020

Jørn Vestergaard