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:** Law firm Ilić & Partners LLP, Matic Kocjančič, Junior Associate

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

**Answer:** Ljubljana, Slovenia

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:** Slovenian legal system does not specifically define the term of "mobile device". It seems that Slovenian legal system rests on the fact that a term "mobile device" is a widely known term and hence needs no definition of its scope. Slovenian Criminal Procedure Act (*Zakon o kazenskem postopku (Uradni list RS, št. 32/12 – uradno prečiščeno besedilo, 47/13, 87/14, 8/16 – odl. US, 64/16 – odl. US, 65/16 – odl. US, 66/17 – ORZKP153,154, 22/19, 55/20 – odl. US in 89/20 – odl. US)*) does however define the term "*electronic device*" in 219.a article. Under definition of electronic device, it includes any and all electronic devices as well as associated devices to it and electronic data carriers.

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.*

*Mobile device seized*

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

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

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

**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?*

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

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

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

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

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

**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.*

**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?*

**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?*

**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?*

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

***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.*

*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.*

**Answer:** The most general privacy right in Slovenian legal system is derived from the 35th Article of Constitution of Republic of Slovenia (***The Constitution***), which stipulates *Protection of the Rights to Privacy and Personality Rights*, as follows: "The inviolability of the physical and mental integrity of every person and his privacy and personality rights shall be guaranteed.". Additionally, 37th and 38th Article of The Constitution, specifically target the question of *Protection of the Privacy of Correspondence and Other Means of Communication*[1] and *Protection of Personal Data*[2]

[1] 37th article of The Constitution:
*The privacy of correspondence and other means of communication shall be guaranteed.*
*Only a law may prescribe that on the basis of a court order the protection of the privacy of correspondence and other means of communication and the inviolability of personal privacy be suspended for a set time where such is necessary for the institution or course of criminal proceedings or for reasons of national security.*

[2] 38th article of The Constitution:
*The protection of personal data shall be guaranteed. The use of personal data contrary to the purpose for which it was collected is prohibited.*
*The collection, processing, designated use, supervision, and protection of the confidentiality of personal data shall be provided by law.*
*Everyone has the right of access to the collected personal data that relates to him and the right to judicial protection in the event of any abuse of such data.*

where the constitution lays out fundamentals for privacy of correspondence and other means of communications and defines a scope when the right of Protection of Privacy may be suspended.

Amendment "J" to Slovenian Criminal Procedure Act from 2009 has regulated the process of gathering evidence from electronic devices. With the latest Amendment "N" from 2019 it broadened the definition of electronic devices, so that it now also includes Cloud storage. But the fundamental prerequisite of having the electronic device in possession in order to be able to access the data remains unchanged. Hence the following answer is separated in two, first one focuses on situation where Mobile device is not seized and the second where Mobile device is seized.

According to Article 150 of Criminal Procedure Act ("CPA"), control of electronic communications (also mobile devices) with eavesdropping and recording can be ordered against the person if there are reasonable grounds for suspecting that he/she has committed, is executing or preparing to commit any of the criminal offenses referred in the second paragraph of this article.

But in order to allow such control over electronic communication devices, it also has to be reasonably concluded that other (less invasive) measures could not be used to collect the relevant evidence. In accordance to Article 150.a of CPA, the authority can obtain data regarding numbers and location of communication devices. With the data obtained on the basis of Article 150.a of CPA, authorities can obtain data from mobile operator. The order of investigative judge, for above described measures, must be issued based on reasoned proposal of the prosecutor. However, in case if the data is locate on the phone or its peripherals, authorities cannot use any technical tools or other means to bypass the phone's security. The access must be granted by the owner of the device by providing the access information. Latter means that without physical seizure, content on the mobile device cannot be neither obtained, nor copied. Although if the access is not granted by the owner, consent of the owner/person in possession is not necessary every time, since the data can be obtained on the basis of a issued court order. But in order to acquire such access the possession of the device is needed, if the mobile device is not seized, the owner cannot be forced to unlock the device. Since the evidential value of the collected data is to be determined by the

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

court during the trial, the investigative measures are always concealed from the suspect as well is the collected data (evidence).

Without physical seizure, the search of mobile device cannot be performed. As mentioned, only data regarding numbers and location of mobile devices can be obtained (Article 150.a of CPA) and electronic communication can be recorded and listened to (Article 150 of CPA). These measures can only be performed on the basis of the order of investigative judge. Data regarding numbers and location of mobile devices (Article 150.a of CPA) and recording and eavesdropping (Article 150 of CPA) can only apply to electronic device of the accused. Nevertheless, as communication is two-sided, data of third party is also obtained, but therefore it has to be processed and stored with utmost respect of the third party's privacy rights.

Regarding the connected databases, if the mobile device is seized, Cloud can be accessed according to Article 219.a of CPA. To obtain data stored in Clouds with servers located outside of the Republic of Slovenia, international cooperation is needed, except if the data is public or if the consent of the person (accused, victim or third person) who can disclose relevant data, is obtained in the sense of Article 32 of Convention on Cybercrime.

On the other hand, when the mobile device is seized and in possession by the police or the court (which has to be done vie court issued order), it can be investigated. Investigation of the device is usually carried out by a appointed professional which is either usually employed by the police or a by an expert, appointed by the court, who must also, in accordance with Article 250 of CPA, carefully examine the subject matter, state precisely everything he/she observes and give his/her opinion impartially and in accordance with the rules of science or expertise. During the investigation the data must (not only can) be copied to another media, with all metadata so that its integrity can be verified anytime later during the proceeding. Although so far there are no limits unto what can be accessed the general rule is that investigation must be done in a way to infringe the rights of victim and other data owners as little as possible, protect the confidentiality of data and to not cause any unnecessary disproportionate damage.

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

Since in case of a issued court order, there is no requirement of the consent of the owner/person in possession of the device, but neither one can be forced (i.e., meaning "*forced by hand*") to unlock the device. The owner/person in possession of the device is obligated to cooperate by law, which also means that he/she is obliged to unlock the device on basis of 223.a art. of CPA.

In case when the device is seized and access to the device is gained, all data (either directly on the device or on connected data storages) can be examined. This is possible due to amendment "N" of CPA from 2019, which broadened the term electronic device, so that now includes also connected data repositories. If a data repository is disconnected later in time after the seizure, it can not be accessed by any other means. The fact that device was previously connected to one repository, is not of enough precedence that connectivity to said repository must be maintained all the time. Summed up, this means, that if the data in the cloud is not connected through the device, it can not be accessed only by the fact that a (possibly) connected device to the cloud was seized.

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:** There is no such protocol. Only obligatory duty of the professional appointed for evidence collection is to create a official record which must include the following:

- Identification of the examined electronic device
- Date and time of start and finish of the examination. For each examination a separate note of date and time must be made.
- List of persons included and present at the examination
- Memo of how the examination was executed
- Memo about findings and other relevant circumstances.

The above is regulated in paragraph 8 of article 219.a of Criminal Procedure Act.

***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:** So far there is no regulation regarding utilization of AI technology in forensics of electronic devices. Processes of evidence collection are in domain of the professional appointed for evidence collection.

***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:** There are specific rules on jurisdiction regarding cybercrime, therefore general rules on jurisdiction apply. Article 30 of Criminal Procedure Act (CPA) states that if someone commits a

criminal offense in Slovenia and abroad (multiple jurisdictions), that the competent court is the court competent for adjudicating on a criminal offence in Slovenia.

The multijurisdictional issues are regulated from Articles 514 CPA onwards, however, if the multijurisdictional issue arises between Slovenia and European countries, the procedure on cooperation and resolving issues arising from the fact that multiple countries have jurisdiction, is regulated in the Law on Cooperation in Criminal Matters with EU Member States, which is a transposition of EU legislation in connection to the matters on criminal cooperation.

***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:** The Law on Cooperation in Criminal Matters with EU Member States in Article 2 states that its provisions shall not apply in regards to cooperation in criminal matters otherwise regulated by directly applicable legal act of the European Union or by an international treaty.

In accordance with the said Article, priority over EIO is given to acts that are directly applicable at the EU level and to individual international agreements that the Republic of Slovenia has concluded with individual countries.

***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:** When it is necessary to carry out procedural acts abroad (eg. obtaining evidence abroad), the competent authority shall request assistance from another country. It shall do so by requesting international legal assistance, drawn up in accordance with applicable international treaties, European law or domestic law. The Republic of Slovenia has concluded 22 multilateral mutual legal assistance treaties (8 within UN and 14 within EU and worldwide) and a larger number of bilateral mutual legal assistance agreements.

The most relevant MLAT, that the Republic of Slovenia has concluded regarding digital evidence and mobile forensics might be Convention on Cybercrime (Treaty no. 185).

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

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

**Answer:** While we understand what the goal of this question is and can see the benefits of such cooperation, the practice is not yet implemented in Slovenia. All professionals are mostly employed in the special police sector, therefore only rarely court appoints professionals. Even in cases when the court appoints a professional it is from a rooster of court approved professionals.

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

***36.* 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:** In Slovenia, the current law governing the protection of personal data is PDPA[3], which is not in line neither with GDPR[4], nor with the Directive 2016/680 ("***Directive***"). While the provisions of GDPR are directly binding, the Directive only sets out the objectives to be achieved by the Member State through the implementation of those objectives into national law. Considering that the new Personal Data Protection Act ("**PDPA2**"), which should implement the GDPR provisions and objectives of the Directive, has not been adopted yet, the Republic of Slovenia is in breach of European law, as the Directive should be implemented into national law by 6 May 2018.

[3] Personal Data Protection Act (*Zakon o varstvu osebnih podatkov,* Official Gazette of the Republic of Slovenia, no. 94/07)

[4] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation; OJ L 119, 4.5.2016, p. 1–88).

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

In such case, the principle of consistent interpretation may be applicable[5]. Also, it may be relevant the decision of the Court of Justice of the EU, in which the court has ruled that certain provisions of directives may exceptionally have direct effect in a Member State, if: (1) the directive has not been implemented into national law or the implementation has been incorrect, (2) the provisions of the Directive are unconditional in substance and sufficiently clear and precise and (3) the provisions of the Directive confer rights on individuals.

The current PDPA regulates legal basis for processing of personal data in public sector (Article 9) and stipulates personal data in the public sector may be processed if the processing of personal data is provided for by law. The law may stipulate that certain personal data may be processed only with the personal consent of the individual. Personal data may also be processed without regard to the foregoing, if this is necessary for the execution of lawful authorizations or obligations of public sector. Since GDPR, in Article 10, only states that the processing of personal data relating to criminal convictions and offenses or related security measures shall be carried out only under the supervision of an official body or if processing is permitted by Union law or the law of a Member State providing adequate safeguards for rights and freedoms of involved subjects and the Directive, in Article 4, provides general principles relating to processing of personal data, paragraph 8 of Article 223.a of Slovenian CPA (more specifically) stipulates that, when the data from mobile device is obtained, the seizure of an electronic device and the protection of data must be carried out in such a way as to infringe the rights of persons other than suspect or accused as little as possible, protect the confidentiality of data and do not cause disproportionate damage due to inability to use the electronic device. Moreover, copies of data which do not relate to criminal prosecution and for which there is no other legal reason that they should be kept, shall be excluded and copies of such data should be destroyed.

[5] Authorities are bound to interpret national law in accordance with the wording and the purpose of the directive.

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

Slovenia will still have to ensure that the provision of Article 10 of the Directive, which regulates the processing of special categories of personal data (data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation), is properly implemented.

Article 5 of the Directive (which is not implemented in Slovenia yet) provides that Member States shall provide for appropriate time limits to be established for the erasure of personal data or for a periodic review of the need for the storage of personal data. Slovenian CPA, in paragraph 7 of Article 223.a of CPA stipulates that data, relevant for the criminal procedure, shall be stored as long as it is necessary for the procedure. Since the mobile device can be seized until identity and integrity of data is ensured, but no longer than 3 months, the above-mentioned copies must be created within 3 months. If the creation of data copies is not possible, the mobile device can be seized and used as long as necessary for the procedure, but no longer that 6 months since the seizure.

Given that the CPA in Article 16 stipulates that the parties to the proceedings are equal, it is necessary to ensure the equality of arms. The acquisition and investigation of data from a mobile device is performed by an expert and the counterparty or the holder of the mobile device often does not have the necessary expertise to assess, whether the aforementioned procedures were performed correctly, in such a way as to ensure the identity of the data. Equality of arms in this area is therefore sought to be ensured by the possibility of the presence of an expert or counsel on the mobile device holders' side, while the mobile device is being secured, the possibility of the accused to present his/her views regarding the evidence extracted via mobile forensics and the fact that evidence extracted via mobile forensics, obtained in unlawful manner (without legal basis, altered…) are not admissible and must be excluded. Non-discrimination regarding digital evidence is to be sought through the demand that extracted data must keep the integrity of original data to be considered as admissible as stated in paragraph 7 of Article 219.a of CPA. In order to ensure integrity of the

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

original data, experts must, with special algorithms, calculate unique digital fingerprint of data and compare calculations of the original data and a copy in order to assess, whether the integrity of the original data is preserved. Moreover, courts should only accept the original proof and a copy or altered version of it only in the absence of the original.

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

## Section 3: Admissibility of evidence before court

***37.* 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:** No. All general rules and guidelines were presented in previous sections.

***38.* 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:** Yes, the criteria for admissibility is the same. Evidence from mobile forensics are a subcategory of general term of evidence, it follows the same procedural rules as any other evidence, albeit material or non-material (i.e testimonies). Therefore, they follow the general rule from art. 18 of Criminal Procedure Act, which regulates the criteria of admissibility of evidence – if the procedural rules (from Criminal Procedure Act) are violated in process of acquiring evidence, such evidence must not be admitted. Additionally paragraph 14 of article 219.a of Criminal Procedure Act lays out sanction of inadmissibility of evidence if they are acquired without order issued by court, against order issued by court or without written consent of the owner of electronic device.

***39.* 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:** If the acquisition of evidence from mobile forensics is not in accordance with the procedural rules, it is inadmissible, without regard to the material value of the said evidence itself. This is due to the fact that same rules apply for evidence from mobile forensics and any and all other types of evidence. Also please refer to answer to question 39.

***40.* 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?*

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

**Answer:** No. As elaborated in Section 1, the Amendment "N" from 2019 broadened the definition of electronic devices, so that the term "electronic device" now also includes data stored in the Cloud storage. The definition of "electronic device" was expanded in order to fully captures any and all possible data that is either on the device itself or the device has access to.

Therefore, it is irrelevant where the actual physical storage medium (on which the Cloud data is stored) is located. Physical storage located in foreign countries does not render the actual data evidence inadmissible.

***41.*** **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.*

According to generally accepted rule; the so-called Best evidence rule; courts should accept only the original proof and a copy or altered version of it only in the absence of the original (see also Supreme court of the Republic of Slovenia decided, in judgement no. I Ips 314/2004 dated 18.9.2006). In the event of the absence of the original evidence, altered version can be admissible if the integrity of original data is kept as stipulated in paragraph 7 of article 219.a of Criminal Procedure Act. Also please refer to answer to question 51.

***42.*** **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:** As provided by paragraph 8 of Article 219.a, the investigation of mobile device must be executed by court expert (professionally qualified person, appointed by a court order). According with the latter, there are technological and methodological standards that must be followed.

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

***43.* 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:** Generally there is case law relating to admissibility of evidence obtained by intercepting electronic communications (Higher court of Ljubljana, no. III Kp 44415/2010 dated 25 October 2013) and relating to admissibility of evidence obtained by searching seized mobile phone (Higher court of Ljubljana, V Kp 13335/2010 dated 28 November 2019 and Supreme court of the Republic of Slovenia, no. I Ips 132/2010 dated 22 December 2011). However, there is no case law thar we are aware of on admissibility of evidence obtained by recovering data from mobile devices (mobile forensics). Also, there is no other similar case law which would be applicable to this question.

***44.* 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.*

**Answer:** In the process of collection, analysis, interpretation and reporting of digital evidence, the integrity of such evidence and possibility of their use in further proceedings must be kept according to paragraph 7 of Article 219.a of CPA. In order to ensure integrity of the original data, experts must, on the basis of hash values, calculate unique digital fingerprint of data. A copy of data that has the same checksum is considered to be identical to the original data and has the integrity of the original data.

According to the before mentioned Article, the investigation must be performed in a way that minimizes intrusion of Personal Privacy Data of other persons, keeps the secrecy of data to the highest standard and mitigates any potential unnecessary damage.

As per paragraph 8 and 9 of Article 219.a of CPA, the investigation of mobile device must be performed by professionally qualified person, who also records the performed search and data obtained. The investigation must be performed on the court premises or other premises, if necessary due to the use of technical means.

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

When the mobile device is seized in order to perform the search, Article 223.a of CPA provides that the data must be transferred and saved on another appropriate data carrier in a way to preserve identity and integrity of data and possibility of their use in further proceedings or an identical copy of the entire data medium is made. Such copy must ensure the integrity of the data.

***45.* 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:** Yes, if the evidence does not pass the test of proportionality in correlation between the evidential value of evidence in certain process and prejudicing the rights of Personal Data Protection of a particular person, it is possible that the evidence becomes inadmissible (See also decision of Higher Maribor court nr. 4993/2014, on 11th of April 2019).

General rule is that the evidential value of each acquired evidence must be greater than the value of protection of one's Constitutional right, in order for said evidence to be admissible.

***46.* 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:** While there is no case law on the question of evidence collection (i.e. whether the procedures utilized to gather the evidence were/were not suitable and hence rendering the evidence inadmissible). Regardless, we found two cases broadly relevant to the above question as described below:

I Kp 24348/2016 dated 29 March 2017:

The Criminal Procedure Act provides that the defendant's counsel is a privileged witness, which means he/she cannot be interrogated as a witness about what he/she was entrusted by defendant as his/her counsel. Such information is covered by the obligation of professional secrecy. Higher court in Koper decided, in judgement no. I Kp 24348/2016 dated 29 March 2017 that evidence, collected through mobile forensics, which provide data on communication between a lawyer and a client

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

must be eliminated *ex officio*, if such data meets the criteria of Article 237 of the CPA in conjunction with the fifth paragraph of Article 154 of the CPA (the information is obtained from a person who may not be heard as a witness).

II Kp 56623/2013 dated 7 August 2014:
In another case, Higher court in Koper in its decision no. II Kp 56623/2013 dated 7 August 2014 found that written consent for the investigation of deceased's mobile device was obtained from his father, whereby he could not replace the will of the deceased but, the protection of privacy rights applies to the living and not the dead man, therefore the privacy in the meaning of Article 219.a CPA can be expected only by a living individual. Consequently, the investigation of the relevant mobile device was not unlawful.

Other than that, there is no other case law on this subject.

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

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

***47.* 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:** Evidence extracted via mobile forensics has equal probative value as any other, more traditional, evidence. Any evidence must be legally admissible and must have adequate probative value. This rule also applies to evidence in digital form, except that the characteristics of the evidence, which are different from some traditional evidence, must also be taken into account. Since it is not difficult to alter digital evidence while extracting it via mobile forensics, it is necessary to take into account 3 elements, including authenticity, integrity and verifiability while assessing probative value of such evidence.

When courts asses admissibility and reliability of such evidence, the rule is, that only data, that kept the integrity of original data, can be used as evidence in the criminal proceedings. Data extracted via mobile forensics that is altered or do not pass the test of integrity cannot be considered reliable.

The investigation of mobile device and extraction of data must be executed by an expert, appointed by the court, who must also, in accordance with Article 250 of CPA, carefully examine the subject

matter, state precisely everything he/she observes and give his/her opinion impartially and in accordance with the rules of science or expertise.

In the Republic of Slovenia, requirements for expert witnesses are stated in Court Experts, Certified Appraisers and Court Interpreters Act[6], which, in Article 16, sets out the requirements that natural persons must meet in order to be appointed as an expert.:

- has relevant expertise and practical skills and experience for a specific field of expertise,
- has a pre-bologna university degree or a completed bologna master's study program,
- is a citizen of the Republic of Slovenia or a Member State of the European Union or a Member State of the European Economic Area and actively speaks the Slovenian language,
- has legal capacity,
- has appropriate personality,
- has at least six years of work experience in the field in which he wishes to work as a forensic expert,
- has not been convicted of an intentional criminal offense prosecuted ex officio, which would make him/her morally unfit to perform expertise, as this could harm the impartial or professional performance of his/her work or the reputation of the court,
- does not perform activities that are incompatible with forensic science,
- has not been dismissed as a forensic expert with the provisions of this Act due to the permanent deprivation of the right to perform the work of a forensic expert.

Moreover, experts must be acquainted with new findings and methods relating their area of expertise, or participate in professional trainings organized by the competent state body, authorized organization, professional association or other professional institution. Expert council shall verify the professionalism of experts, after the expiration of five years from the date of appointment and after the expiration of each subsequent five years.

[6] Court Experts, Certified Appraisers and Court Interpreters Act (*Zakon o sodnih izvedencih, sodnih cenilcih in sodnih tolmačih,* Official Gazette of the Republic of Slovenia, no. 22/18)

In general, experts are supervised by an expert council, who may impose disciplinary measures if the expert violates his obligations or the rules and principles of the profession. Such measures should ensure that experts act professionally and that their work and findings are compliant with standards and can be presented in court in a consistent manner.

**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:** There is no such case law so far. See also answer to question 47.

***48.*** **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:** According to decision of Constitutional court of the Republic of Slovenia no. Up-106/05-27 dated 2.10.2008, the Constitution, in the first paragraph of Article 37, which ensures the secrecy of letters and other media, protects freedom of communication, which ensures. the protection of the individual's interest, that without one's consent no one becomes acquainted with the content of the message transmitted through any means of exchanging or transmitting information. The field of protection of communication privacy extends to letters and other media (e.g .telephone, fax, or computer). The subject of communication protection should be interpreted broadly, so that it includes content of the communication and information about telephone calls (meaning data from the telephone memory printout).

Based on that, the process of handling with and storing digital evidence is laid out in paragraph 7 of article 219.a of Criminal Procedure Act. It stipulates that integrity of original data must be kept and data must be made available for usage in further proceedings. Investigation must be executed in a manner that minimizes intrusion of Personal Privacy Data of other persons, keeps the secrecy of data to the highest standard and mitigates any potential unnecessary damage.

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

As per paragraph 8 and 9 of article 219.a of Criminal Procedure Act, the investigation must be carried out by a professional (which is either professional employed by the police or any other professional appointed by court). The investigation must take place on court premises or exceptionally on other locations if this is necessary due to technological requirements (i.e. at the premises of appointed professional).

Higher court in Maribor emphasized, in judgment no II Kp 34177/2012, dated 5 February 2019 that evidence obtained with digital forensics must ensure the integrity of the original data. In the absence of the principle of data integrity as a fundamental principle of computer forensics, the seventh paragraph of Article 219.a and the first paragraph of Article 223.a of the CPA is violated.

***49.* 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:** The generally accepted rule in the criminal procedure theory and case law is that the court should accept the best (direct) evidence. However the Supreme court of the Republic of Slovenia decided, in judgement no. I Ips 314/2004 dated 18.9.2006, in which the court was presented with recordings of intercepted telephone conversations, which were not original, but subsequently processed and partially erased by Center for forensic investigations, that the taking of evidence that deviates from this rule does not mean that the evidence is inadmissible in the sense of point 8 of paragraph 1 of Article 371 of the CPA, but can only affect the assessment of the credibility of evidence.

Due to the fact that evidence produced with mobile forensics must keep the integrity of original data, the court, in order to verify the integrity of original data was not lost by subsequent processing of Center for forensic investigations, also read written records of unaltered telephone conversations and concluded that integrity of altered records was kept and evidence were admissible.

So far there is no other judicial precedence available in Slovenia.

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

***50.*** **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:** As decided by Constitutional court of the Republic of Slovenia in judgement no. UP 729/03, U I 187/04 dated 11 December 2004, the right to a defence through counsel is an essential element of the right to a fair trial. Its purpose is to ensure *de facto* equality of arms in criminal proceedings. In order to respect the principle of equality of arms, the suspect or the accused has the right to be present with his counsel during criminal proceeding and also during the seizure of the mobile device. During the latter, an expert may be also present with the suspect/accused, which further ensures the equality of arms, given that this process requires specific expertise.

Among others, equality of arms is also ensured by the fact that the accused can always present his/her views regarding the evidence extracted via mobile forensics and the fact that evidence extracted via mobile forensics, obtained in unlawful manner (without legal basis, altered…) are not admissible and must be excluded.

There is no other or similar case law on this topic.

***51.*** **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:** Unfortunately, no; except for expert witnesses, who must be professionals appointed by the court and have to have a licence from their field of expertise.

***52.*** **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?*

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

**Answer:** In accordance with paragraph 7 of Article 223.a of CPA, copies of seized data are stored as long as it is necessary for the procedure. Due to the fact that mobile device can be seized by authorities until identity and integrity of data is ensured, but no longer than 3 months, the above-mentioned copies must be created within 3 months. If the creation of data copies is not possible, the mobile device can be seized and used as long as necessary for the procedure, but no longer that 6 months since the seizure.

***53.* 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:** According to Article 6 of the Directive GDPR (which is still not implemented in Slovenia), Member States shall provide for the controller, where applicable and as far as possible, to make a clear distinction between personal data of different categories of data subjects.

According to Slovenian CPA, the seizure of mobile device does not require active participation and such measure may be imposed against anybody who is in possession of such device, including against the suspect, the victim, persons who may have the status of a privileged witness or persons who are relatively incapable of testifying.

Slovenian CPA stipulates that the mobile device holder must, on the request of the authority, take immediate necessary action to prevent the destruction, alteration or concealment of data and allow access and provide passwords in accordance with paragraph 3 and 7 of Article 219.a of PCA. The duty to act to the request of the authority does not apply to the suspect, person who cannot be heard as a witness according to Article 235 of CPA or to a person who has denied testimony in accordance with Article 236 of CPA. The CPA also stipulates that special attention must be paid to the rights of persons other than suspect and accused, since the seizure of an electronic device and the protection of data must be carried out in such way as to infringe as little as possible the rights of before mentioned persons.

As stated in paragraph 4 of Article 223.a of CPA, when securing data obtained from a mobile device, the owner of the device, his representative or lawyer, or an expert invited may be present.

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

In the process of investigating a mobile device, the court must ensure that the deadlines, within which the device and the obtained data can be kept, are observed, as mentioned in question no. 54.

## 5.1 The Prosecution

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

**Answer:** No. The evidence is handled and stored by the court.

## 5.2 The Court

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

**Answer**: All approaches and methods utilized during the investigation of mobile device are in the sole domain of appointed professional by the court. See also answer to question 52, 47.

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

**Answer:** Applicable criminal law does not differentiate between assessing the evidential value of evidence obtained via mobile forensics in comparison to other evidence. See also answer to question 51 ("*The court should accept the best direct evidence*").

## 5.3 The defendant and defender

***57.* 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**: The Republic of Slovenia still needs to implement the GDPR Directive, from which it follows, the right to rectification or erasure of personal data and restriction of processing (Article 16). Moreover, on the basis of the Directive, certain information should be made available and given to the data subject (Article 13) and data subject should be granted the right of access to processed personal data (Article 14). Provisions relate manly to the purposes of the processing, for which the personal data are intended, the categories of recipients of the personal data, including in third countries or international organisations, the categories of personal data concerned, communication of the personal data undergoing processing and of any available information as to their origin, etc. Nevertheless all mentioned rights can be limited in order to avoid obstructing official or legal inquiries, investigations or procedures, moreover, Article 18 stipulates that Member States may provide for the exercise of the rights referred to in Articles 13, 14 and 16 to be carried out in accordance with Member State law where the personal data are contained in a judicial decision or record or case file processed in the course of criminal investigations and proceedings. That means that the Directive is fully applicable to criminal proceedings, but since Member States'criminal procedural codes already provide for rules on information, access, rectification, erasure and restriction of processing, the provision recognizes such codes as correct transposition efforts[7].

In view of the above, the Slovenian CPA is considered to be sufficient basis for the regulation of the defendant's and his/her defender's rights to access and to make copies of the acquired mobile evidence. According to paragraph 4 of Article 223. a of CPA, when securing and copying data obtained from a mobile device of the defendant, his representative or lawyer, or an expert invited

[7] J.Sajfertand, T.Quintel: Data protection directive (EU) 2016/680 for police and criminal justice authorities, p. 7

may be present. CPA does not provide for the presence of the owner of the device, his representative, lawyer or expert, during the investigation process, nor does it provide any provisions related to obtaining copies of the acquired mobile device. However, as stated in paragraph 8 of Article 219.a of CPA, a report of the investigation shall be made and shall also include information on any persons involved and present in the investigation; the findings of the investigation, the manner of executing the investigation and other relevant circumstances.

Higher court in Maribor decided in its judgement no. V Kp 45306/2015 dated 9 October 2019 that regarding the presence of the suspect and witnesses in the investigation of the electronic device, the legislator clearly assessed that the presence of the subject and witnesses in the investigation of electronic devices was not necessary and that the results of the investigation of electronic devices could always be reviewed from the protected data from the electronic device, while reasonably pointing out that this is an identical situation as in the case where the police would inspect the seized documents. Namely, it only confiscates them, draws conclusions that can always be verified or refuted by re-examination or by a different interpretation of the seized documents, and the possibility of asserting that the communication was in fact different as concluded from the produced evidence, is therefore given to the defendant.

## 5.4 Witnesses

***58.*** **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:** In accordance with paragraph 6 of Article 223.a of CPA, the seizure of an electronic device and the protection of data must be carried out in such way as to infringe as little as possible the rights of persons other than suspect or accused, protect the confidentiality of data and do not cause disproportionate damage due to inability to use the electronic device.

As provided in paragraph 9 of Article 223.a of CPA, copies of data which do not relate to criminal prosecution and for which there is no other legal reason that they should be kept, shall be excluded and copies of such data should be destroyed.

Regarding the capability of witnesses to testify, the request of the authority to take immediate necessary action to prevent the destruction, alteration or concealment of data and allow access and provide passwords in accordance with paragraph 3 and 7 of Article 219.a of PCA does not apply to person who cannot be heard as a witness according to Article 235 of CPA or to a person who has denied testimony in accordance with Article 236 of CPA.

So far there is no other judicial precedence available in Slovenia

## 5.5 The Victim

***59.* 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:** As in the case of the investigation of the electronic device of a witness, the investigation of the electronic device of the victim must be executed in a way to infringe the rights of victim as little as possible, protect the confidentiality of data and do not cause disproportionate damage due to inability to use the electronic device. Also copies of data, found on victim's mobile device, which do not relate to criminal prosecution and for which there is no other legal reason that they should be kept, shall be excluded and copies of such data should be destroyed. Because the victim can be heard as a witness, the request of the authority, to take immediate necessary action to prevent the destruction, alteration or concealment of data and allow access and provide passwords in accordance with paragraph 3 and 7 of Article 219.a of PCA, is applicable to the victim.

In criminal proceedings, the prosecutor acts on behalf of the victim, who may rely on the evidence obtained via mobile forensics. The same applies if the victim takes over the prosecution himself.

So far there is no other judicial precedence available in Slovenia.

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:** Every aspect has been sufficiently covered in scope of the above questions and related answers.