USE OF THE MVT MOBILE PHONE FORENSIC ANALYSIS SOFTWARE

DATA PROTECTION NOTICE

This processing operation refers to the use of the Mobile Verification Toolkit (MVT)[1] software tool by the EDPS, while carrying out forensic investigation on mobile devices. MVT is a collection of utilities designed to facilitate the consensual forensic acquisition of iOS and Android devices for the purpose of identifying any signs of compromise, namely by the Pegasus spyware. MVT is developed and released by the Amnesty International Security Lab[2] and is implemented for use at the European Data Protection Supervisor (EDPS) under the terms of the software license[3] (an adaptation of Mozilla Public License v2.0[4]).

We process your personal data based on Regulation (EU) 2018/1725 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by the Union institutions and bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (hereinafter "the Regulation").

We provide you with the information that follows based on Articles 15 and 16 of the Regulation.

Who is the controller?
The controller is the European Data Protection Supervisor (EDPS).

EDPS responsible department or role: Technology & Privacy Unit, EDPS-IT@edps.europa.eu

For more information on the EDPS please consult our website: https://edps.europa.eu

What personal data do we process and who has access to this personal data?
The analysis carried out by the MVT software tool is performed on the phone's backup, where it processes various types of personal records typically found on a mobile phone, such as

- Details about the backup and the device, such as name, phone number, IMEI, product type and version
- Records of HTTP requests and responses performed by applications as well as system services
- Address book
- Records of incoming and outgoing calls, including from messaging apps such as WhatsApp or Skype
- Browsers' favourites as well as cache and history of URL visits

[1] https://docs.mvt.re/en/latest/ / https://github.com/mvt-project/mvt
[2] https://www.amnesty.org/en/
[3] https://docs.mvt.re/en/latest/license/
[4] https://www.mozilla.org/MPL

- Details about attachments sent via SMS or iMessage
- Information about installed apps
- SMS and WhatsApp messages containing links
- Details about user interactions with installed apps
- Cache of apps which requested access to location services
- Records containing a history of data usage by processes running on the system
- Timeline of configuration profile operations. For example, it should indicate when a new profile was installed from the Settings app, or when one was removed
- Records of opened tabs in Safari
- Cache of Apple user ID authentication
- Phone shutdown records
- List containing services and the permissions they were granted or denied
- Record of Operating system updates
- Local stored files created by all applications
- Records of resources loaded by different domains visited

You can find a detailed explanation of the records extracted and processed, as well as the reasons for processing such records, at the following web pages:
Apple IOS: https://docs.mvt.re/en/latest/ios/records/
Android: https://docs.mvt.re/en/latest/android/methodology/

Where did we get your personal data?
The personal data is collected upon exporting the phone's backup to the MVT laptop, for the sole purpose of processing with the MVT for performing the forensic analysis.

The forensic analysis is performed by the EDPS-IT, in the presence of the owner of the phone (user), using a laptop computer that has no connection to any network. The phone is connected to the laptop computer, using a cable, and an image of the phone (backup) is transferred to the laptop computer.

When exporting the image of the phone (backup) to the laptop computer, the user inputs a one-time use password that is used for encrypting the backup. Once the backup is complete, the phone is disconnected from the laptop computer and the user must type again the one-time use password to decrypt the backup. This one-time use password is never again needed or used in this analysis process.

The EDPS-IT uses the MVT tool set to perform the analysis. During the analysis, the data is processed by the MVT tool set and the results of the analysis are shown on the screen and saved in report files. No personal data or record are ever shown in the screen and the data processing is performed in the laptop computers' volatile memory. Volatile memory's contents are permanently lost when the laptop computer is shutdown therefore, because the personal is processed in volatile memory, it is never permanently saved to any other location. Once the analysis is complete, the phone's image (backup) is permanently erased from the laptop computer.

The report files created by the MVT tool do not contain personal data and are kept for evidence, after being renamed to contain a reference to the user and date, and encrypted with a secure password managed by the EDPS-IT.

Upon completion of the analysis, the result is shown to the user, the report files are securely encrypted and the laptop is shutdown, thereby permanently erasing every trace of personal data.

Why do we process your personal data and under what legal basis?

Personal data are processed in order to carry out the forensic analysis, for the purpose of identifying any signs of compromise, namely by the Pegasus spyware.

Participation to the forensic analysis is voluntary. The lawfulness for this processing is based on Article 5.1.(d) of the Regulation ("consent") .

How long do we keep your personal data?

All personal data is immediately erased upon conclusion of the analysis. The analysis takes a few minutes (the exact duration depends on the amount of data contained on the backup).

What are your rights regarding your personal data?

You have the right to request access to your personal data and to relevant information concerning how we use it. You have the right to request rectification your personal data. You have the right to ask that we delete your personal data or restrict its use. We will consider your request, take a decision and communicate it to you.

You can send your request to the EDPS by post in a sealed envelope or use our contact form on the EDPS website (see section on contact details below).

How to withdraw your consent and the consequences of doing this

You have the right to withdraw your consent at any time. Please note that withdrawing your consent does not affect the lawfulness of processing based on consent before its withdrawal. Should you wish to withdraw your consent, please inform the EDPT-IT (edps-it@edps.europa.eu).

You have the right to lodge a complaint

If you have any remarks or complaints regarding the way we process your personal data, we invite you to contact the EDPS DPO (see section on contact details below).

You have, in any case, the right to lodge a complaint with the EDPS as a supervisory authority: https://edps.europa.eu/data-protection/our-role-supervisor/complaints_en.

Contact details for enquiries regarding your personal data

We encourage you to contact us using the EDPS contact form, selecting 'My personal data' as the relevant subject: https://edps.europa.eu/node/759

If you wish to contact the EDPS DPO personally, you can send an e-mail to DPO@edps.europa.eu or a letter to the EDPS postal address marked for the attention of the EDPS DPO.

EDPS postal address: European Data Protection Supervisor, Rue Wiertz 60, B-1047 Brussels, Belgium

You can also find contact information on the EDPS website: https://edps.europa.eu/about-edps/contact_en.