

Consolidated version of the conducted by VMobile Data Protection Impact Assessments concerning the data processed and collected within the PATHEARN Project

1. Systematic description of the processing operations and the purposes of the processing. Main parameters of the Data Protection Impact Assessment (DPIA)

1.1. Purpose of PATHEARN

The purpose of PATHEARN is to create a database of a) (**Stationary Objects**) IoT devices, and multiple moving and stationary objects (e.g., road signs) and/or b) detailed surrounding area images database i.e., anonymized exterior photos of streets, roads, neighborhoods, localities, parks, gardens, etc. (**Imagery**); where a) and b) are both collected together with GPS location and timestamp (and are collectively referred to as the **Data**), in order to provide services to third parties (clients), such as statistics, data verification, traffic analysis, etc. (the **Project**).

Data can be collected through the purpose-built Pathearn application <https://pathearn.ai/> (the **PATHEARN app**) and/or through the purpose-built Pathearn application for CCTV cameras from a) users via their mobile devices (**Private Users**); b) VMobile partners (**B2B Users**) and/or c) internal channel of our staff (where a), b) and c) are collectively referred to as **users**).

Collected Data is used for the purposes like:

- Provision of services to data analysis companies
- Selling anonymized data
- Providing predictive analytics after data analysis and processing done by artificial intelligence.

The Project does not envisage any trade of personal data.

The benefits of the Data processing are related not only to the successful implementation of the Project:

- The strict technical and organizational measures as well as the innovative technology used by VMobile are strong guarantees for the data protection and the information security of the whole Project and its ecosystem too;
- The large-scale implementation of the Project would help to optimize the urban environment such as reducing emissions, mobility management, optimizing traffic, parking areas, optimizing fuel consumption or tolls, solving problems of the nature of ecology and biology, by monitoring the determination of growth zones, etc.

1.2. Types of data and their processing

There are basically two categories of data processed:

- Data of data subjects related to the implementation of the Project** – Private Users, B2B Users and/or our staff (with official e-mails). The data are following the principle of minimization and are in the amount of strictly necessary – email and password;
- The Data required for the purposes of the Project.**

The data on i. are processed through the functionalities of the PATHEARN app.

NB! The information that is automatically collected from the user device/s, such as geolocation data and current time, is not stored or used in a way that can be associated with any user in a personally identifiable way. This means in practice that the received by us geolocation data and time stamp is

in no way linked to the geolocation and time of the users. This is so for the following reasons: (i) as said, the users provide us only with the minimum data for registration purposes and the use of the PATHEARN app – email and password; (ii) when they enter their email address and password at the PATHEARN app, the PATHEARN app automatically transforms this data (i.e., hashes it) into a generated ID that is displayed in place of the user's email address in all our systems. The PATHEARN app authenticates the users via their email and password, but we see only the generated ID. Therefore, we do not link the email with the data the users provide us with via the PATHEARN app, including the location of the user and/or the location of others around the user. There is also no link between the email of the user and the generated ID, as the described process of transformation cannot be reversed.

The Data on ii. are processed as follows:

Re Stationary Objects - In case the PATHEARN app (via mobile devices or CCTV cameras) catches any road signs or other Stationary Objects, VMobile automatically receives such Data (i.e., cropped picture of the Stationary Object at hand without any surroundings) plus the current time, and the GPS coordinates of the it. The process does not involve any video recording or taking comprehensive photos, outside the searched Stationary Objects. Users do not have access to any of this information. Anyhow, as the location of the Stationary Objects and the personal data of the users are not linked, as described hereabove, in this case the Project includes neither users' data processing, nor data processing of any other data subjects.

Re Imagery - Via the camera screen of the user's mobile device, but opened through the PATHEARN app, photos in real-time are taken. Users do not have access to these photos, cannot save them, and cannot use them for personal purposes. If a user wishes to send the photos taken to our software by pressing the button to upload the photos, they are anonymized through the device, thanks to the artificial intelligence of the PATHEARN app, by blurring people's faces. The following information is sent to our server in an encrypted channel: the User's photos with human faces blurred, GPS coordinates, time of shooting. The uploaded information is automatically deleted from the device. Upon receipt of the Data, a second stage of automatic anonymization by Pathearn immediately begins, checking for missed non-blurred individuals or other identifiable information. Strategic objects, irrelevant content (e.g. interior photos) and/or any other information that would constitute personal data or is unsuitable for the purposes of the Project would be also detected manually and deleted.

Against the Data, Private Users, as well as some B2B Users receive points that they could exchange for cryptocurrency.

Generally, the collected Data is not stored or visualized on the devices and/or in the PATHEARN app. In the event of a loss of connection to our servers, a limited amount of Data (which failed to be transferred to the server, although the sending process was initiated before the connection was lost) remains stored locally in the application (a hidden folder of the respective device) until the connection is restored. After the connection is restored and the user initiates uploading, the Data will be sent to our servers and immediately deleted from the device. The user does not have access to the Data in any case.

Users data, as well as the Data obtained from them (whether Stationary Objects or Imagery), are stored on our servers/cloud space, which are located on the territory of Bulgaria (and Turkey – for the purposes of Turkish data and processing) in observance of all technical and organizational measures provided by VMobile and adequate to the needs of the Project. Imagery Data is stored in anonymized version. The data of the users is stored in encrypted and pseudonymous versions.

1.3. Data Storage

The storage of the user's data depends on the use of the PATHEARN app e.g., accounts that are not used at all for 24 months and have no accumulated points or accounts that have been used and have accumulated points but after that the user ceases activity for 24 months, would be deleted and the data on it would not be stored by VMobile. Accounts that provide for not real Data will be also deleted (e.g., Data from live streaming, Data from old pictures, etc. Data that is not gathered in the manner described herein). In other cases, the data is processed and stored while the PATHEARN app is used.

The storage of the Data depends on the legitimate interest of VMobile to collect the database of the Project. However, deletion on grounds of relevance is made on a period of max. 5 years (inaccurate or not up-to-date Data).

We use the following criteria to determine how long we retain personal information: (a) our relationship with the users, such as if there is an open account or a pending request, (b) legal obligations to retain personal information for certain purposes, such as to maintain transaction records, and (c) other obligations or considerations relating to the retention of personal information, such as (but not limited to) contract requirements, litigation holds, investigations, or statutes of limitation.

1.4. Role of the users and the individuals with installed cameras

The persons with PATHEARN app accounts (including those with installed cameras) are its users. As such, they do not have access to the Data through their device or through the PATHAERN app portal.

The access to the Data extracted from VMobile, the protection of the Data, as well as the control over the Data is entirely and exclusively on VMobile. Users do not have any real possibility to process the Data (within the GDPR meaning of the definition of "processing"); there is no way they to implement specific technical and organizational measures against this Data and/or to assist VMobile at the request of Data subjects or in case of data breach. The entire data processing cycle is focused on the actions and measures of VMobile, as a data controller. For this reason, such users cannot meet the concept of "data processors", even though they are somehow involved in the process of collecting the Data.

1.5. Necessity to conduct a DPIA

The manner of processing of VMobile Data does not imply or aim in any way their accumulation with other data, as well as the identification of certain data subjects. Where Stationary Objects is collected the Data storage and encryption mechanism is designed in a way that it does not involve the collection of personal data at all. Where Imagery is collected the Data is received already anonymized, and a process of re-verification and anonymization is carried out after receiving it. There is no possibility of reverse engineering. Access to all Data is strictly limited on a need-to-know basis and performance of official duties to several designated for this purpose persons - staff of VMobile.

Nevertheless:

- The review of the criteria for performing of DPIA for Imagery shows that the Project might include large-scale and systematic monitoring of certain public areas and large-scale data processing.
- The Project will be implemented through the use of innovative technologies - algorithms for statistical analysis, neural network (i.e., artificial intelligence).

- The nature of the Project does not allow all data subjects to be widely informed about the data processing.
- The Project also envisages the use of a mobile application (for iOS and Android devices) – namely the PATHEARN app.

Taking into account the GDPR rules, all various guidelines and opinions of the European Data Protection Board (the **EDPB**) and analyzing the amount of information to be processed by VMobile, it was decided a DPIA to be conducted for the processing of Imagery (the "**DPIA**") in order to comply with the principles of privacy by design and privacy by default and further to comply with the EDPB's principle: "*in cases where it is not clear whether a DPIA is required, the WP29 (now EDPB) recommends that a DPIA is carried out*"¹.

2. Assessment of the necessity and proportionality of the processing operations in relation to the purposes

- VMobile has a **legitimate interest** (Article 6, paragraph 1, item f) of the GDPR) to collect the Data. The database is key to the implementation of the Project and the provision of the Data to VMobile's clients (as fully anonymized Data). By applying the principles of processing a minimum amount of data and their proportional use in order to implement the Project, the data processing is completely sufficient, but also strictly necessary for the purposes of VMobile. VMobile also performs balancing tests to determine whether the purposes and manner of processing take precedence over the rights of data subjects (see p. 5 hereunder).
- The processing of data (email and password) with respect to the registration and/or the use of the PATHEARN app is based on the **legitimate interest** of VMobile to run the PATHEARN app and also on the agreed by the users Terms of Use (i.e., **contractual basis** for processing).

3. Assessment of the risks to the rights and freedoms of data subjects. Defined risk level.

- With regard to the systematic and large-scale monitoring of the Imagery, the DPIA demonstrates that the way the Data is processed does not include any actual and material monitoring of data subjects. The photos are stored and received from the users in an anonymized version that does not allow identification and/or profiling of persons. A second automatic anonymization check is performed by VMobile immediately after the receipt of the photos. In addition, photos with strategic objects and/or inappropriate content are further manually detected and deleted. It is possible that a limited amount of personal data may be processed (received by VMobile) only during the period between receiving the anonymized data from users and the verification phase, which aims to remove missed non-anonymized individuals, as well as other elements from the images that could potentially identify data subjects. In this regard, no residual risks to data subjects are disclosed in relation to the monitoring activity.
- The Project will be implemented through the use of innovative technologies for which all necessary information security measures have been taken, including for the implementation of the targeted application for data collection – i.e., the PATHEARN app.
- The nature of the Project does not allow all data subjects to be informed about the processing in accordance with all GDPR requirements. For this reason VMobile will provide all necessary information documents on publicly accessible places such as its online platform, the PATHEARN app and other appropriate places.

¹ <https://ec.europa.eu/newsroom/article29/items/611236>

The DPIA shows an **acceptable average to low level of risk** as the measures in place to protect the rights and freedoms of data subjects have been implemented satisfactorily. The Data is collected in an anonymized form, without the possibility of reverse engineering.

The DPIA shows that the processing of the Data could not lead to the identification of certain data subjects or that this could happen with a disproportionate effort in extremely rare cases and with the availability of additional information/data.

VMobile has ensured that the persons through whom the Data will be collected do not have any access to it, that the Data is not stored on separate devices (except for a short period of time in case of broken server connection) and that their control and protection is entirely a VMobile's responsibility.

Controls are provided to ensure the confidentiality, integrity, and availability of all personal data, encrypted channels for its retrieval, pseudonymization and/or anonymization for their use and transmission.

All internal rules and policies of VMobile would be updated in view of the implementation of the Project and the data flows in it.

4. Measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate GDPR compliance taking into account the rights and legitimate interests of data subjects and other persons concerned

The impossibility for direct notification of all data subjects for the processing of the Data was determined as an activity with residual risk. VMobile takes additional measures for organizing an information campaign in this regard, in addition to all data protection documents created for the users of the PATHEARN app and the online platform. For this reason, we are also publishing this consolidated version of the DPIA - so that stakeholders can get acquainted in as much detail as possible with the processing activities.

With respect to the Imagery the determined information security is adequate to the needs of the Project - the Data is received anonymized (with blurred persons), a subsequent check and re-anonymization is performed (with additionally blurred data), access to the Data is limited, the transmission of the Data to the VMobile server is carried out by encrypted channel, the work with the various data streams is strictly regulated.

When information is collected, it is extracted from the image (i.e., with respect to Stationary Objects) or sent directly (i.e., with respect to Imagery) in the PATHEARN app and sent directly to the VMobile server. SSL (Secure Sockets Layer) and TLS (Transport Level Security) encryption are used. Buffer Stored Data (a certain amount of Data, in case of no connection to the VMobile server) in the device is also encrypted and transferred to the VMobile (and deleted from the device) immediately after connection is restored and user initiate uploading. Users do not have access to the Data. In addition, when Imagery mode is used to capture images of the environment all images are stored in a device-protected system folder that the mobile operating system does not allow users to access. When the user clicks the upload button, the anonymization process begins. The process goes as each image is anonymized, sent to the server and deleted from the user's device.

5. Balancing test for the lawful basis for the Data processing

Before relying on the lawful basis of legitimate interests, VMobile needed to assess:

1. **Purpose Test:** Is VMobile pursuing a legitimate interest?
2. **Necessity Test:** Is the intended processing necessary for that purpose?

3. **Balancing Test:** Do the data subject's rights and interests override the legitimate interest of VMobile?

Purpose Test

The implementation of the project can help to optimize the urban environment such as reducing harmful emissions, managing mobility, optimizing traffic, optimizing fuel consumption or tolls, solving problems of the nature of ecology and biology, through monitoring of determining growth zones, etc. Various business groups are interested in the realization of all these goals.

These are all legitimate interests of businesses and organizations.

Necessity Test

Controllers also need to demonstrate that the processing is necessary for the purposes of the legitimate interest identified. This does not mean that it has to be absolutely essential, but it must be a targeted and proportionate way of achieving the legitimate interest.

VMobile deems the processing to be targeted and proportional as:

- It is proportionate to the needs of gathering the Data for a database.
- The analysis conducted by VMobile would be extremely difficult (if not impossible) and time-consuming to replicate by other means.
- The Data is gathered by processing a minimum amount of personal data, usually anonymized at the point it is received by VMobile.

Balancing Test

The Balancing Test requires VMobile to take into account: (a) the data protection and privacy rights of the data subject, (b) the fundamental rights of the data subject and (c) the more general interests of the data subject, and ensure that such rights/interests do not override VMobile's interests.

VMobile has considered the following in relation to the Balancing Test:

- The Data is gathered by processing a minimum amount of personal data, usually anonymized at the point it is received by VMobile.
- The Data to be gathered would not appear to override any privacy rights or fundamental rights as it is used is minimal and it is not of any sensitive or special categories of personal data.
- The processing is not related to the processing of children's data or data related to other vulnerable groups.
- The processing does not concern the personal or professional life of the data subjects.
- The processing is not of any nature that a personal data breach could jeopardize the health or safety of any data subjects, or otherwise cause them any substantial harm.
- No negative impact is expected from the technologies used for Data processing. Adverse impacts could occur in the almost non-existent situations of technological failure with much additional effort and additional data availability.

Overall Assessment

VMobile holds the view that legitimate interests can be relied on when the three Tests are applied and balanced among one another.

The DPIA was conducted in compliance with the requirements of GDPR, the applicable EU and Turkish national legislations, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default², Working Party 29 Opinion on the use of location data with a view to providing value-added services³, Guidelines 07/2020 on the concepts of controller and processor in the GDPR⁴, and all other applicable laws and regulations.

² https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en

³ https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2005/wp115_en.pdf

⁴ https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_en