MOBIDOT GENERAL PRIVACY & DATA PROTECTION POLICY

1.   Introduction

Mobidot B.V. is a Dutch business service provider with a focus on measuring and influencing personal mobility behaviour via the Smartphone. Mobidot is based in Enschede and registered in the trade register of the Chamber of Commerce under number 57131422.

Because personal mobility data is central to our products and services, we pay a lot of attention to privacy and good data management. As a processor of privacy sensitive data, we consider it of great importance that users and clients can rely on us. This means that we deal responsibly with data and specific Personal Data. The implementation of our products and services therefore complies with all relevant EU and Dutch legislation. In particular, the General Data Protection Regulation (EU2016 / 679, and its Dutch counterpart 'Algemene Verordening Gegevensbescherming', hereafter "AVG"). We also comply with the guidelines and recommendations from the Dutch Data Protection Authority and the European Data Protection Board (EDPB).

With regard to data management and the protection of privacy, we use a privacy-by-default and privacy-by-design policy and approach that lead to measures in the areas of:
- Design and implementation of services and technical systems, interfaces and infrastructure ('Development');
- The execution of these services within project or service frameworks for Clients, whether or not in collaboration with other Parties ('Operation'). This concerns in the broadest sense the mapping ('tracking') and analysis of the mobility behaviour of participants (our 'Users'), informing, advising and rewarding Users with regard to mobility choices and supportive communication and management processes such as helpdesk and reporting to Clients .

This document provides an overview of our policy and the measures we take and have already taken.

2.   Privacy and data protection approach

In order to protect the data of (potential) Users and to guarantee privacy, our privacy-by-default and privacy-by-design approach translates into the following three measure areas:

Focus on minimization
- We use data that can identify an individual only to the extent necessary from an explicit and legitimate purpose of the Operation.

- Data is no longer stored by us than necessary for the purpose of the Operation or stated from legislation and is only shared between the Parties insofar as necessary for the purpose of the Operation.

Focus on enforcement

- We make agreements with the Client and other Parties involved in the Operation concerning the processing of Personal Data, in which the roles of the Controller and the Processor are clearly defined and allocated. We jointly record these agreements in one or more processor agreements. This also applies to business Partners, whom we contract to execute our obligations through sub processor agreements.
- Users give explicit permission before we collect and process personal data. We do this in a transparent and privacy friendly manner with unambiguous opt-ins. Parts of every opt-in are a specific privacy statement and the Terms of Use associated with an operation. When a User wants to stop using our products or services, all data about this User will be completely and promptly removed to the extent that no legal obligations are in force.
- Data that can identify an individual are protected and shielded by appropriate technical, organizational and procedural security measures. Guarantees are set against unauthorized access to data. Data leaks are proactively reported to the Dutch Data Protection Authority.
- We have established a Data Protection Officer who supervises compliance with our privacy policy and data protection measures.

Focus on transparency

- Depending on the Operation, we consider ourselves Controller or Processor in the sense of the Personal Data Protection Act.
- We keep a register of processing activities.
- We are transparent and concrete to every (potential) User about their privacy, which data is collected and processed and which rights the User has. This information is standard part of our consent and opt-in procedures. Our general privacy policy is publicly available.
- Users are informed when we use Partners or third party services. As sub-processors, Partners are obliged to protect the personal data of the Users. Third party services, for example from Google or Apple, are not part of our privacy policy and Users individually agree with their terms and conditions.
- We provide a central point where (potential) Users can file complaints and questions about privacy and exercise their right to access their data and correct errors.

3.   Privacy design and implementation rules

Where we speak about core service, we are talking about the processing of privacy sensitive (location) data of Users within the Operation. Where we speak about support services, we are talking about personal communication and assistance to a (potential) User. A potential User can only become a User via explicit consent with the applicable conditions at the Operation. A User can

always withdraw his / her consent, after which we will remove all privacy-sensitive data of this person from our systems.

Minimize data need

The categories of Personal Data that are collected and processed in our Operation are:
- Account information
  Collective goal: to provide access to (the use of) our products and services. To personalize our products and services. To inform our Users.
  Key data: Username (E-mail address), residential and / or work addresses, interests and preferences.
- Contact details
  Collective goal: to provide support for specific individual questions or problems of Users with respect to our services.
  Key data: E-mail address and / or telephone number
- Mobility data
  Collective goal: to collect information on travel behaviour and enriching it to a travel profile. To provide insights into travel behaviour and effects. To give travel advice. To support rewarding of Users for displayed travel behaviour.
  Key data: smartphone sensor (GPS, Wi-Fi and Accelerometer) traces of a user linked to times ("trips"); collected feedback from a User.
- Log data
  Collective goal: to analyse and improve the performance and use of our products and services.
  Key data: usage data / analytical data

With each Operation a specific privacy statement applies in which the Controller, all specific Parties involved, the purpose of the processing and the explicit list of the collected and derived data are described.

Data retention periods

Mobidot stores Personal Data for as long as necessary from the purpose of the Operation and as determined by the Controller, unless it is obliged by law to keep certain Personal Data for a longer period. All collected and derived Personal Data will be deleted from the systems of Mobidot within three months after Operation end. After a year of inactivity, a User and all of his / her individual Personal Data will be removed from the Mobidot systems. Both a Client, in its role as Controller, as an individual User can instruct Mobidot to remove Personal Data of an individual from its systems and / or to deactivate (the) User (s), for example if a User leaves service, no longer meets certain conditions or no longer makes use of the Mobidot services. Mobidot will carry out all related requests within one working month.

Restrictive application and proportionality

The collected data is
- processed and enriched to determine and map certain travel behaviour within the framework of the Operation and to prepare incentives.
- aggregated and anonymised for monitoring and reporting
- checked for fraud analysis
- kept by us until a date in accordance with the Operation or as determined by a User.

Personal data, unless Mobidot is or becomes obliged to do so by law or a court order, will not be shared with third parties outside Mobidot or the partnership of Parties from which the Operation takes place. Personal data will only be released to third parties after a User has explicitly given permission or instructions for this.

We do not intentionally collect Personal Data from children under the age of 16. If it appears that we have collected Personal Data from someone who is younger than 16 years and no consent has been given by parents or guardian, the relevant account will be closed immediately and the Personal Data will be deleted.

Security of information
- We take administrative, process, technical and physical measures to protect Personal Data against misuse, as well as unauthorized access, disclosure, alteration and destruction. Our security meets at least the criterion of an "appropriate security level" as defined in Article 32 of the AVG. We carry out a Data protection impact assessment (DPIA) on a regular basis.
- All Personal Data is stored and processed in a secure data centre in the Netherlands with physical and logical access security including organizational control. The data centre of Mobidot is equipped with a reliable infrastructure that guarantees the continuity of the service. Mobidot uses data centre facilities from the Dutch company Previder (www.previder.nl). This data centre is ISO 27001, 14001 and 9001 certified. In the context of privacy and data protection, Mobidot has concluded appropriate SLA contracts with Previder.
- Logical and physical access control to the ICT systems. Mobidot has digitally secured its System Environment with a hardware-based firewall and monitors its System Environment for unauthorized access and intrusion. Mobidot will do everything that can reasonably be expected to do to prevent unauthorized physical and digital access to its System Environment and the data by unauthorized persons. It does this, among other things, by equipping its System Environment with recent operating systems and the latest (security) patches, which are recommended and supported by the suppliers for use in the Mobidot System environment. In connection with the reliable use of the software used, Mobidot also strives for the optimal combination of all used software components.
- Mobidot is obliged to process the Personal Data of Users properly and carefully. Mobidot guarantees that the personnel of Mobidot and anyone else who is engaged by Mobidot

adheres to the requirements of the AVG, or in the provisions of the Exemption Decree and the provisions made by the Client, if and in so far as they are involved in any way whatsoever in the processing of Personal Data. Management of the Mobidot System Environment is carried out and monitored by authorized Administrators employed by Mobidot bound by an integrity contract and confidentiality statement;

- Only a limited group of delegated Administrators designated for this purpose and assigned by the Controller has access to the System Environment. These delegated Administrators, which are authorized by Mobidot Administrators can configure certain settings, are allowed to make certain changes to the service setup and are able to generate certain statistical overviews within the Operation. Each delegated Administrator receives an individual, unique user ID and password from Mobidot. The password is only known to the delegated Administrator himself. Only the Administrator himself and the Mobidot Administrators can change the password. A password is for individual use only. The delegated Administrator is responsible for keeping the granted password or the password confidential. Mobidot Administrators may revoke the rights of a delegated Administrator on the instructions of the Controller.
- Data leaks are reported proactively to the Dutch Data Protection Authority.
- The communication between apps, data processing infrastructure and Mobidot websites is via secure connections;
- Mobidot ensures the splitting of data (pseudonymisation), whereby personal data (who) and mobility data (such as location trails) are separated in the data processing process.
- Non-aggregated exports from the databases are stored with access security.
- We use audit trails to be able to verify who, when and with what authorization, has had access to data.
- Security incidents can be reported at any time at support@mobidot.nl

Anonymization

Mobidot establishes anonymous travel movements for monitoring and reporting and to gain an insight into the travel movements in the Netherlands at an aggregate level. This statistical information can be useful for transport operators, government, civil society organizations and research organizations to improve accessibility, develop mobility policies, monitor or evaluate and encourage sustainable transport. Mobidot analyses and visualises the captured mobility data and uses this data to improve mobility in the Netherlands towards more convenience, healthier and more active travel and more sustainable modes of transport.

We think it is very important to emphasize that the data we use for this collect cannot be traced back to an individual. We anonymize all data about travel movements and delete all references to an individual. This process cannot be reversed. Anonymisation is achieved by aggregating and randomizing collected location tracks and derived information from Users. Randomization includes:

- Cutting away 0-200 meters at the beginning and end of captured routes;

- Deleting user information so that, for example, it is no longer traceable that the car trip from A to B was performed by the same person on Tuesday as the journey from C to D on Friday;
- Shifting data in time with a randomly determined offset between -30 ... +30 minutes

Informing the User

We are transparent and concrete to each (potential) User about their privacy: which data is collected and processed, for whom and for how long and what rights the User has. For this purpose, a privacy statement is available for each specific Operation, specifying the purpose and commitment of our service, scope and relevant Parties. The most important implementation rules within these statements that we communicate to the Users in advance are:

1. You have control over your provided or measured personal data at all times.
2. We collect only those data that are necessary for the purpose of the Operation and for which there is a legal basis.
3. Only aggregated and anonymised data can be shared with third parties. Personal data, with the exception of a court order, will never be provided to third parties without your permission.
4. You have the right to view all data recorded about you and obtain it (in a standard format). If you believe that data is incorrectly recorded, you can request Mobidot to change or delete it.
5. You can stop using our services at any time. After one (1) year of inactivity, your personal data will be proactively removed.
6. You can request to delete all your personal details at any time you wish. This will be carried out within a working month and insofar as no legal obligations are in force. If the latter is the case, Mobidot will inform you of this.
7. If you are of the opinion that Mobidot does not handle your data correctly, you can make this known through our complaints procedure. If this does not lead to a solution, you can always use your right to file a complaint with the Dutch Data Protection Authority or to appeal to a competent court.
8. If you have questions about our Privacy Policy, you can always contact us by e-mail at privacy@mobidot.nl

4. Privacy and security auditing

In the continuation of fraud audits, a Client can carry out audits to check whether we use the privacy and data protection rules and statements carefully and correctly.

In addition, we have a general accountability to comply with the AVG. To this end, a data protection officer (DPO) has been appointed by Mobidot and registered with the Dutch Data Protection Authority. This person can be contacted via the contact details below.

Changes to this Privacy Policy

Mobidot reserves the right to change its Privacy Policy from time to time. We do not limit the rights of a User under this Privacy policy without his / her consent. We will post changes to the Privacy

Policy on our website and, if the changes are significant, we will provide a more prominent notice to the Users.

5.   About Mobidot and contact

Mobidot B.V. is a Dutch company and innovative specialist in measuring and influencing personal mobility behaviour via the Smartphone.

Mobidot B.V

Address:	Colosseum 44
	7521 PT Enschede
	The Netherlands
Chamber of Commerce:	57131422
Website:	www.mobidot.nl
E-mail:	info@mobidot.nl
Support:	support@mobidot.nl
Privacy questions, complaints and incidents:	privacy@mobidot.nl
Data Protection Officer:	dr. Ir. ME. Bijlsma
Telephone number:	+31 (0)6 51514135