

## Privacy Notice – XXIMO UK

Version ENG 1.0 – March 2023

### 1. XXIMO

XXIMO UK Limited (**XUKL, we, us**) is a subsidiary of XXIMO Holding B.V. (**XXIMO**). XUKL handles the operations and services provided in the UK. XXIMO has its own privacy notice, available [here](#).

### 2. This notice

The purpose of this privacy notice (**Privacy Notice**) is to provide you with detailed information about how and why we collect and process your personal data in the UK. This might be when you ask us to provide an XXIMO Mobility Card or other relevant services to you or access [our website](#) (together, the **Services**), or where your employer/organisation has contracted with us to provide our services to you. It also applies where you interact with us by email, via our website, social media, or by any other means.

### 3. Our role

XUKL is a “controller” under the UK General Data Protection Regulations (**GDPR**). This means that we are responsible for deciding how we hold and use personal information about you. Where we receive your personal data from XXIMO or another of our group companies, they may also be a controller of your personal data.

We have appointed a data protection officer (**DPO**). If you have any questions about this Privacy Notice, please contact our DPO at [privacy@xximo.com](mailto:privacy@xximo.com).

### 4. What personal data do we collect?

‘Personal data’ means any information about you from which you can be identified. It doesn’t include data where your identity has been removed (known as anonymous data).

We may collect, use, store, and transfer different kinds of personal data about you, grouped together as follows:

- Identity Data includes name, title, sex/gender, username or similar identifiers including customer number, date of birth, and formal/photo ID.
- Contact Data includes address, email address, telephone numbers and other contact information provided to us.
- Professional Data includes employer, industry, staff number, and position.
- Financial Data includes bank information such as IBAN, credit card details, and PAN-number.
- Regulatory Data includes origin of assets, UBO register data, PEP information, and sanctions data.
- Technical Data includes internet protocol (IP) address, your login data, operating system or browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform, and other technology on the devices you use to access our Services.
- Usage Data includes information about how you use our Services, including information about your transactions, purchases, travel arrangements, tolls, accommodation and all other usage information.
- Marketing and Communications Data includes your preferences in receiving marketing from us and our third-parties and your communication preferences.
- Any other information you or your employer/organisation provides to us.

We also collect, use, and share aggregated data such as statistical or demographic data for any purpose. Aggregated data could be derived from your personal data but is not considered personal data in law as this data will not directly or indirectly reveal your identity.

Some of the information we collect about you via payment information may indicate 'special categories of personal data' as defined by Article 9 of the GDPR but we do not process such special category data itself for any purposes.

Where we need to collect personal data by law, or under the terms of a contract we have with you or your employer/organisation, we may not be able to perform the contract and provide our Services if you fail to provide the data.

## 5. How do we collect your personal data?

Your personal data comes to us from a few different sources:

1. Direct interactions – you may provide the personal data to us when you interact with us. Eg., by filling in forms, corresponding with us, or interacting with us online whether via our website or not.
2. From your organisation – we might receive your personal data from your employer/organisation when they contract with us for our Services. In order to find out how your employer/organisation handles your personal data, please refer to their privacy notice or equivalent documentation.
3. From third-party merchants – we collect some of your personal data (including Usage Data) from companies or organisations where you use your XXImo Mobility Card (such as in a petrol station or hotel).
4. From our group companies – XUKL is part of a global group of affiliated companies with some overlapping operations. This means that we sometimes need to share personal data with each other. Therefore, some of the personal data about you may be provided to us by one of our group companies, including XXImo.
5. Automated technologies or interactions – as you interact with our Services, including using our website, we automatically collect some personal data, including Technical Data. We also receive some personal data from cookies and other similar tracking technologies. Please see further cookie information by clicking the cookie link at the bottom right corner of the Website, or within the cookie consent banner upon initially visiting the Website.
6. From other third-parties – we receive personal data from analytics providers (such as Google and Piwik PRO).

## 6. How do we use your personal data?

We only use your personal data when the law allows us to. Most commonly, that will be in the following circumstances:

- Where we need to perform the contract we are about to enter into or have entered into with you or your employer/organisation.
- Where it is necessary for our legitimate interests (or those of a third-party) and your interests and fundamental rights do not override those interests.
- Where we need to comply with a legal obligation, including complying with financial regulations.

Generally, we do not rely on consent as a legal basis for processing your personal data. Where we *do* rely on your consent as a lawful basis, we may process this personal data until you withdraw such consent. However, if you give us permission, we will process your personal data in order to inform you

about other services we offer and will keep this personal data until you unsubscribe. Note that we will send you push/local notifications from time to time without your permission where these are necessary for the Services, such as when you need to refuel, or when you are approaching your spending limit.

We need to process your personal data to provide our Services and comply with the law. This means administrative purposes, such as collections and handling disputes, drawing up invoices for you or your employer/organisation, storing data for you or your employer’s obligations to keep records, creating and presenting informational reports, communicating with your employer/organisation, making the Services usable, improving the quality of the Services and preventing misuse or security incidents.

IDT Financial Services Limited (“IDT”) is the issuer of the card associated with our Services. Accordingly, IDT is a joint controller of some of your Personal Data as it relates to, and is required for, the administration and operation of the card. A copy of IDT’s privacy policy may be found at <https://idtfinance.com/privacy-policy/>

## 7. Purposes for which we will use your personal data

Note that we may process your personal data on more than one lawful basis depending on the specific purpose for which we are using your data. Please contact us if you have any questions.

Purpose / Activity	Type of data	Lawful basis
To comply with administration obligations including tax laws	Identity Data, Contact Data, Financial Data	Legal obligation
Mandatory customer identification under financial legislation	Identity Data, Contact Data, Professional Data, Regulatory Data	Legal obligation
To provide our Services	Identity Data, Contact Data, Professional Data, Financial Data, Technical Data, Usage Data	Performance of a Contract, Legitimate Interests
To comply with transaction monitoring obligations	Identity Data, Financial Data, Usage Data	Legal obligation
To market our Services to you	Identity Data, Contact Data	Consent
To improve our Services	Identity Data, Contact Data, Professional Data, Usage Data	Legitimate Interests

Please be aware that where your Usage Data reveals any special categories of personal data, this will only be processed for the purpose of providing you or your employer/organisation with the Services and complying with our legal obligations.

## 8. How long will you keep my personal data for?

We will only retain your personal data for as long as reasonably necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, regulatory, tax, accounting or reporting requirements. We may retain your personal data for longer in the event of a complaint or where we reasonably believe there is a prospect of litigation in respect of our relationship with you.

To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can

achieve those purposes through other means, and the applicable legal, regulatory, tax, accounting, or other requirements.

For example, we keep most personal data relating to direct communications between us and you for a period of 6 months, but we have to keep some administrative data for 10 years for tax regulatory purposes.

## 9. Who do we share your personal data with?

We may share your personal data with the parties set out below for the purposes set out above.

1. Processors – we engage third-parties to assist us in providing the Services and comply with our obligations. Note that in some cases these processors collect the personal data from you on our behalf. In all cases, we have strict GDPR-compliant agreements in place with our processors to ensure that we stay responsible for the lawful processing of your personal data. These processors may include:
  - analytical software (this includes Piwik PRO and Google Analytics, set up in such manner that no personal data is shared with Google.);
  - BIN sponsors (VISA licensee);
  - customer relation management software;
  - third parties with which you use the XXImo Mobility Card;
  - hosting providers;
  - marketing;
  - software developers;
  - support;
  - card manufacturer;
  - software for customer identification;
  - software for transaction monitoring;
  - XXImo Mobility Card providers.
2. Employers/resellers – if you use our Services as an employee or if our Services are otherwise made available to you through your employer, we need to share personal data with them in order to provide our Services.
3. Our professional advisors – we need to share some personal data with our legal, tax, financial, and other business advisors in order to comply with the law, protect our interests, and continue to provide our Services.

We may also sometimes need to share your personal data with government bodies, regulators, or other third-parties as strictly necessary to comply with the law or a legal request by an authority. In this case, as in all the cases above, we will only share as much personal data as is absolute required for the relevant purpose.

## 10. How do we keep your personal data safe?

We have in place appropriate technical and organisational security measures for the processing of your personal data. We comply with industry accepted standards to protect your personal data, both during the transmission thereof and as soon as we have received the personal data. We have taken the following measures in any case:

- we have implemented physical and technical measures and management procedures designed to prevent unauthorised access, loss or misuse of personal data as much as possible;
- security-sensitive personal data, such as account passwords and other payment-related identifiable information, is sent in encrypted form;

- security-sensitive information (including your password) is stored in encrypted and/or hashed form where possible;
- we restrict the internal access to personal data to employees who require the information to perform their duties. Our employees are bound by confidentiality obligations;
- our information management systems are set up in such manner that employees who are not authorised to examine specific information or personal data do not, in principle, have access to such information;
- our servers are located in a secure environment in data centres in the Netherlands. You only have access to the front end of our servers and only by logging in by means of a username and password. You are responsible for keeping your login details safe;
- the personal data is backed up on a frequent basis.

### 11. International transfers

We sometimes need to transfer your personal data outside of the UK. This includes where we share personal data with our group companies, including XXImo. Many of our external third-parties are also based outside the UK so their processing of your personal data will involve a transfer of data outside the UK. Whenever we transfer your personal data out of the UK, we ensure a similar degree of protection is afforded to it by ensuring at least one of the following safeguards is implemented:

- Only transferring your personal data to countries that have been deemed to provide an adequate level of protection for personal data; or
- Where we use certain service providers, we may use specific contracts approved for use in the UK which give personal data the same protection it has in the UK.

Please contact us if you want further information on the specific mechanism used by us when transferring your personal data out of the UK.

### 12. Your rights

Under certain circumstances, you have rights under data protection laws in relation to your personal data. They won't always apply – for example, you only have the right to erasure where it is not overridden by a legal obligation to retain the personal data for a legal obligation. However, you may have the right to:

- Request access to your personal data
- Request correction of your personal data
- Request erasure of your personal data
- Object to processing of your personal data
- Request restriction of processing your personal data
- Request transfer of your personal data
- Withdraw consent

We may need to request specific information from you to help us confirm your identity and ensure your right to access your personal data (or to exercise any of your other rights). This is a security measure to ensure that personal data is not disclosed to any person who has no right to receive it. We may also contact you to ask you for further information in relation to your request to speed up our response.

### 13. Lawful basis definitions

- **Legitimate Interest** means the interest of our business in conducting and managing our business to enable us to give you the best service/product and the best and most secure

experience. We make sure we consider and balance any potential impact on you (both positive and negative) and your rights before we process your personal data for our legitimate interests. We do not use your personal data for activities where our interests are overridden by the impact on you (unless we have your consent or are otherwise required or permitted to by law). You can obtain further information about how we assess our legitimate interests against any potential impact on you in respect of specific activities by contacting us.

- **Performance of Contract** means processing your data where it is necessary for the performance of a contract to which you are a party or to take steps at your request before entering into such a contract.
- **Comply with a legal obligation** means processing your personal data where it is necessary for compliance with a legal obligation that we are subject to.