

XXIMO PRIVACY STATEMENT

Version 3.0 - October 2023

Table of Contents

1. XXImo	2
2. General	2
3. Categories of Personal Data Collected & Purposes	2
3.1 Visitors on our website	3
3.2 Users of our services - general	5
3.3 Users of the XXImo VISA mobility card	7
3.4 Users of the XXImo OV-chipkaart	8
3.5 Users of the XXImo EV charging token	9
3.6 Users of workstation management and/or mileage registration	9
3.7 Apple and/or Google Pay users	10
3.8 YOR24 Platform	11
3.9 Newsletters	12
3.10 Events	13
3.11 Contact XXImo	14
3.12 Persons covered by the XXImo screening	14
3.13 Corporate clients and contacts of our corporate clients	15
3.14 Applicants	16
4. Processors	17
5. Sharing your personal data	17
6. Protecting your personal data	17
7. Links to third-party sites	18
8. Your rights as a data subject	18
9. Period of Limitation	19
10. Contact	20

1. XXImo

The moment you visit our website, contact us or use our services, we process your personal data. In this privacy statement, we will explain how we collect, use, and secure your personal data.

XXImo provides mobility services and XXImo's activities are divided among several entities including:

1. XXImo Holding B.V.
2. XXImo Financial Services B.V.
3. Stichting Client Monies XXImo Financial Services
4. XXImo B.V.
5. XXImo Belgium B.V.
6. XXImo GmbH
7. XXImo UK Ltd.
8. XXImo France
9. XXImo Czech

The privacy role of the entities varies by the type of processing activities. Their roles and implications for each processing activity will be explained below:

The entities listed under 1 to 3 act as, unless explicitly stated otherwise in this privacy statement, joint controllers with:

1. **XXImo B.V.** if you visit our Dutch website, contact us regarding our Dutch office, or use our services through a customer who has entered into a contract with XXImo B.V.
2. **XXImo Belgium B.V.** if you visit our Belgian website, contact us regarding our Belgian branch, or use our services through a customer who has entered into a contract with XXImo Belgium B.V.
3. **XXImo GmbH** if you visit our German website, contact us regarding our German office, or use our services through a customer who has entered into a contract with XXImo GmbH.
4. **XXImo UK Ltd.** if you visit our UK website, contact us regarding our UK office, or use our services through a customer who has contracted with XXImo UK Ltd.
5. **XXImo France** if you visit our French website, contact us regarding our French office, or use our services through a customer who has contracted with XXImo France.
6. **XXImo Czech** if you visit our Czech website, contact us regarding our Czech website, or use our services through a customer who has contracted with XXImo Czech.

The entities have entered into a joint controller agreement with each other. It is agreed therein that the entity specified above for each country will act externally and towards you as a contact person. Nevertheless, you may always contact any of our other entities. They will ensure that your request reaches the right entity and is handled appropriately.

2. General

XXImo processes your data stored on servers in the European Economic Area ("EEA") unless otherwise stated.

We may change the provisions of this privacy statement from time to time. If we do so, we will notify you of the changes. However, we also recommend that you occasionally check yourself whether the privacy statement has changed.

3. Categories of Personal Data Collected & Purposes

There are several ways in which we may collect your personal data. Below, we describe which personal data we process and for what type of service. The overview and description is as follows:

- 3.1. Visitors to our website
- 3.2. Users of our services – general
- 3.3. Users of XXImo VISA mobility card
- 3.4. Users of XXImo OV-chipkaart
- 3.5. Users of XXImo EV charging token
- 3.6. Users of workplace management and/or kilometre registration
- 3.7. Users of Apple and/or Google Pay
- 3.8. YOR24 Platform
- 3.9. Newsletters
- 3.10. Events
- 3.11. Contact with XXImo
- 3.12. Persons subject to XXImo screening
- 3.13. Business customers and contacts of our business customers
- 3.14. Applicants

3.1 Visitors on our website

Cookies are placed on our website for targeted advertisements. Below we describe what type of data is processed by the cookies, and also what data is processed for website security purposes. Additionally, the data we process in case you contact us is described under Section 3.10 and the data processed if you use our platform is described under Sections 3.2 to 3.7.

A. Essential cookies

In order to display our website and/or our portal to you, we process your cookie preferences. The processing is necessary to pursue our legitimate interest to be able to display our website to you in the desired way and to comply with our legal obligations; this forms the legal basis of our processing. Personal data thus collected will be processed until 2 years from the time of collection. We use a cookie banner on our website to gather your preferences. In case you do not choose to opt-in for the cookies, you can continue to use the website without any cookies (except the strictly necessary cookies) being placed on your system(s).

B. Non-essential cookies

- Preference cookies: Preference cookies enable a website to remember the information that changes the way the website behaves or looks, like your preferred language or the region that you are in.
- Statistics cookies: Statistics cookies help website owners understand how visitors interact with websites by collecting and reporting information anonymously.
- Marketing cookies: Marketing cookies allow the creation of user profiles for advertising and similar marketing purposes. The following cookies are marketing cookies:

a) Piwik Pro

To improve our services, we process the path the visitors take on our website (customer journey) by collecting web statistics.

Our legal basis for processing is your consent. Piwik Pro stores the data in Germany. The following are the processing activities:

- _pk_id#: Collects statistics on the user's visits to the website, such as the number of visits, average time spent on the website and what pages have been read. The cookie expires after 1 year.

- _pk_ses#: Used by Piwik Analytics Platform to track page requests from the visitor during the session. The cookie expires after 1 day.

b) Google Ads cookie(s)

To improve our marketing campaigns, we process the browsing patterns of visitors on the XXImo website. Google Ads (a third-party advertising service provided by Google LLC ("Google")) employs cookies and similar tracking mechanisms to gather insights into the same. The data amassed remains anonymous to XXImo and does not enable us to personally identify individual users. We use these to effectively communicate our products and services to a broader audience and raise awareness about our innovative solutions by providing valuable information to potential customers.

Our legal basis for processing is your consent. These cookies expire after 3 months and XXImo does not store any personally identifiable data beyond this. Google processes the data within and outside the EEA (such as in the United States) and for its own purposes, however, the applicable EU-US Data Privacy Framework approved by the European Commission requires Google to adequately secure your personal data. We have set up Google Ads in such a way that we cannot see any personal data. If you want to know more about what Google does with your personal data, you can consult the Google privacy policy at <https://policies.google.com/privacy>.

c) Meta cookie(s)

To improve our advertisements, we use Meta cookies for delivering a series of advertisement products such as real-time bidding from third-party advertisers. We use cookies to count the number of times that an ad is shown and to calculate the cost of those ads. We also use cookies to measure how often people do things, such as make a purchase following an ad impression. For example, the "_fbp" cookie identifies browsers to provide advertising and site analytics services.

Our legal basis for processing this is your consent. These cookies expire after 3 months and XXImo does not store any personally identifiable data beyond this. Meta processes the data within and outside the EEA (such as in the United States) and for its own purposes, however, the applicable EU-US Data Privacy Framework approved by the European Commission requires Meta to adequately secure your personal data.

d) LinkedIn cookie(s)

We use LinkedIn cookies to improve our marketing campaigns. These cookies expire after 3 months and XXImo does not store any personally identifiable data beyond this. LinkedIn processes the data within and outside the EEA (such as in the United States) and for its own purposes, however, the applicable EU-US Data Privacy Framework approved by the European Commission requires LinkedIn to adequately secure your personal data.

Our legal basis for processing is your consent. We have set the LinkedIn cookies in such a way that we cannot see any personal data as the data remains pseudonymised. If you want to know more about what LinkedIn does with your personal data, you can consult the LinkedIn privacy policy at <https://www.linkedin.com/legal/privacy-policy>.

e) Hubspot

We use Hubspot, a marketing and sales automation tool to achieve our inbound strategy. This tool allows us to generate, manage, and maintain quality potential customers in an automated way. Hubspot processes the data within and outside the EEA (such as in the United States) and for its own purposes, using Amazon Web Services (AWS). However,

the applicable EU-US Data Privacy Framework approved by the European Commission requires Hubspot to adequately secure your personal data.

The cookies used for this include necessary (essential) cookies, and analytics, functionality, and advertising cookies. Details regarding these cookies can be obtained from XXImo's cookie statement on our website. Our legal basis for processing the data collected by Hubspot is your consent.

f) Vimeo

We use Vimeo to embed videos on our website. Vimeo uses cookies for the same and our legal basis for processing is your consent. The following are the cookies used:

- __cf_bm: This is a necessary cookie and it expires after 1 day. This cookie is used to distinguish between humans and bots. This is beneficial for the website, to make valid reports on the use of their website.

3.2 Users of our services - general

When you use our mobility and/or other services, we process your personal data. What personal data we process depends largely on which services you use. Below, we describe what personal data we process when you use our mobility services. The description for the specific services follows later in this privacy statement. Please note the distinction between the user of our services (usually the cardholder) and the customer (the business party with whom we contract).

A. Accounts for the end-users of our services

If you use our services, we will process your personal data to create an XXImo account for you. This allows us to link your use of services to you as a person. Below, we describe which personal data we process when you have a user account with XXImo. The exact data we process depends on the data we obtain from you and your employer or reseller. Therefore, we may not process all the information we list below.

Our legal basis for the data processing is, on the one hand, that the processing is necessary for the preparation of a monthly invoice, which is necessary for the execution of the (employment) agreement you have concluded with your employer (who is our client, directly or indirectly through a reseller). In addition, we also process this personal data because the processing is necessary for our legitimate interest to be able to fulfil our agreement with our client, administration purposes, handle disputes, prepare reports, communicate with you, and your employer and provide you with our services.

- Name
- Address
- Account number
- XXImo customer number
- Date of birth
- Gender
- Nationality
- Phone number
- Email address
- Vehicle registration number (if mobile parking, refuelling and/or charging is activated)
- Card number
- Employer
- Staff number
- Function and department
- Language

- User Identifier (a file to associate your identity across various platforms)
- The services your employer purchases from us
- Username
- Manager ID

If you do not wish the above data to be processed by us, please reach out to us at privacy@xximo.com and we will take this into account as far as possible. However, please take into account that some data is necessary for the provision of the services. If you refuse to provide us with such necessary data, you may be prevented from using our services or we may restrict your access to our services.

For the non-mobility users who use our services to provide manager approvals, we may also process the relevant categories of personal data as described above.

We store this data for 2 years from the date the relationship between XXImo and the customer ceases to exist or the end-user leaves the customer's employment.

B. Account for our customers and their contacts

If you are a XXImo customer or you act as a XXImo customer contact person, we will create a customer account for you. Below we describe which personal data we process about you when you have a XXImo customer account. We obtain this personal data from you, a colleague of yours or your employer. Our basis for the data processing is that the processing is necessary for our legitimate interest to be able to properly fulfil our agreement with our customer, administration purposes, handle disputes, prepare reports, and communicate with you.

- Name
- Gender
- XXImo customer number
- Language
- Email address
- Phone number

If you do not wish the above data to be processed by us, please reach out to us at privacy@xximo.com and we will take this into account as far as possible. However, please take into account that some data is necessary for the provision of the services. If you refuse to provide us with such necessary data, you may be prevented from using our services or we may restrict your access to our services.

We store this data for 2 years from the date the relationship between XXImo and the customer ceases to exist or the contact person leaves the customer's employment (the old contact person's data will be retained for 6 months from the date their employment ceases).

C. Security

The website and online environment of account holders are secured. To make the security work, we process your IP address for up to 6 months after it has been processed unless an incident has occurred, in which case your IP address is processed for up to 6 months after the incident has been dealt with. The legal basis for this processing is that the processing is necessary to pursue our legitimate interest in securing the website and your account.

D. Administration

Based on tax laws, we have a legal obligation to maintain the records. We must keep our financial records for 7 years after the financial year in which the invoice was issued. In our financial records, we process our customer's company name, business address, business account number, Chamber of Commerce number and other information stated on the invoice (such as amounts and transactions). The data is provided by you or your contact person, except for the invoice information generated by us.

3.3 Users of the XXImo VISA mobility card

If and when you use our VISA mobility card, we process your personal data. Below, we describe what categories of personal data we process when you use our VISA mobility card. Our legal basis for such processing, on the one hand, is that the processing is necessary for preparing the monthly invoice, which is necessary for the execution of the (employment) agreement you have concluded with your employer (who is our customer, directly or indirectly through a reseller). In addition, we also process this personal data because the processing is necessary for our legitimate interest to fulfil our agreement with our client, for administrative purposes, to settle disputes, to prepare reports, to communicate with your employer, and to provide you with the VISA mobility card.

We store this data for a maximum of 7 years from the date of collection.

A. Delivering the card

To provide you with the VISA mobility card, we process your name, address, card number, and who your employer is. We receive this information from your employer.

B. Transactions

If you use our VISA Mobility Card to pay, we may receive and process an encrypted version of your credit card PIN from VISA. We cannot read this PIN. In addition, we receive and process your PAN number from VISA. This is the 16-digit number on the front of the credit card. We store this PAN number in encrypted form.

Furthermore, we process your transaction data. We link this transaction data to your account, as described in Section 3.2. above. Exactly which data is processed depends on the type of transaction you make. For example, we only process your parking duration if you use the VISA mobility card to park.

- Transaction ID
- Price of transactions
- Date and time of the transactions
- Products purchased (e.g. type of fuel, travel class)
- Where the product was purchased (company name and location)
- Parking duration and location
- The location where the toll payment is made
- XXImo tag for electric charging (we share this personal data with the electric charging supplier you use)
- Duration of electric charging session and address/location of the electric charging session (we receive this data from the electric charging supplier you use)
- Pick-up and delivery points when using taxis, a shared car, or a shared bike
- Destination and departure points for air and rail travel
- Date and time of air and rail travel
- Other data given for the purpose of the trip
- Hotel location and date of stay
- Departure and arrival point when using public transport

We receive this personal data from the company or organisation where you use the VISA mobility card (such as a petrol station, charging station, hotel, or car parking). We share the relevant transactional categories with VISA to the extent required.

We exchange with your employer and/or reseller your name, employer, employee number, and all card details. To find out how your employer or reseller handles your personal data, please refer to your employer's and/or reseller's privacy statement.

C. Transaction monitoring and sanction screening

Certain financial legislations (such as the Dutch Financial Supervision Act (“Wft”), Anti-Money Laundering and Counter-Terrorism Financing Act (“Wwft”) and the Sanctions Act) require us to monitor transactions for identifying unusual transactions. This monitoring is automated, but in the event an unusual transaction is flagged, an XXImo employee will investigate the transaction and determine whether or not the transaction is unusual. We will only monitor data that we are legally obliged to monitor. We will keep the data for up to 5 years after the date of the transaction. We must report any unusual transactions to the competent supervisor, such as the Financial Intelligence Unit in the Netherlands. We are not allowed to inform you about this in advance. We process the following data for compliance purposes:

- Name of the cardholder (not in the case of anonymous cards)
- XXImo customer (this is usually your employer)
- Customer number
- Type of transaction
- Transaction ID
- Card authorisation data
- Card authentication data (including PIN information)
- Card ID
- Amount
- Receiver
- Location of the receiver

If you carry out transactions with the VISA mobility card in your name, we check whether you are on a sanctions list. We have a legal obligation to carry out this check. This is only done for the relations (customers, UBOs, authorised representatives, and cardholders) of XXImo Financial Services B.V. This check is automated, but if you are on the sanctions list, we will share your data (if we are legally obliged to do so) with the competent supervisor, such as the financial supervisor in the country where the transaction took place and the financial supervisor in your country of residence. We will not inform you if we are required to do so. For these purposes, we process the following data:

- Full first names
- Last name
- Place of birth
- Date of birth
- Place of residence

3.4 Users of the XXImo OV-chipkaart

If and when you use our XXImo OV-chipkaart, we process your personal data. We describe what categories of personal data we process when you use our XXImo OV-chipkaart. Our legal basis for the data processing, on the one hand, is that the processing is necessary for preparing a monthly invoice, which is necessary for the execution of the (employment) agreement you have concluded with your employer (who is our customer, directly or indirectly through a reseller). In addition, we also process your personal data because the processing is necessary for our legitimate interest to fulfil our agreement with our client, for administrative purposes, to settle disputes, to draw up reports, to communicate with your employer, and to provide you with the OV-chipkaart.

We store this data for a maximum of 7 years from the date of collection.

A. Card creation and delivery

To create and deliver the XXImo OV-chipkaart, we process your name, address, and date of birth. We share the name and the date of birth with Translink. We received this data from your employer.

B. Transactions

We process your transaction data as described below. We link this transaction data to your account, as described in Section 3.2 above. We receive this transaction data from Translink.

- Check-in and check-out locations
- Date and time of check-in and check-out
- Travel class
- Cost of the trip

3.5 Users of the XXImo EV charging token

If and when you use our XXImo EV token, we process your personal data as set out below. Our legal basis for the data processing, on the one hand, is that the processing is necessary for preparing a monthly invoice, which is necessary for the execution of the (employment) agreement you have concluded with your employer (who is our customer, directly or indirectly through a reseller). In addition, we also process your personal data because the processing is necessary for our legitimate interest to fulfil our agreement with our client, for administrative purposes, to settle disputes, to draw up reports, to communicate with your employer, and to provide you with the EV token.

We store this data for a maximum of 7 years from the date of collection.

A. Card creation and delivery

To create and deliver the XXImo EV Token we process your name, address, and date of birth. We received this data from your employer.

B. Transactions

We process your transaction data as described below. We link this transaction data to your account, as described in Section 3.2 above. We receive this data from Greenflux.

- Electric charging locations
- Date and time of loading transaction
- Cost of the trip
- kWh for electric charging

3.6 Users of workstation management and/or mileage registration

If and when you use workplace management and/or kilometre registration, we process your personal data as described below. Our legal basis for the data processing, on the one hand, is that the processing is necessary for preparing a monthly invoice, which is necessary for the execution of the (employment) agreement you have concluded with your employer (who is our client, directly or indirectly through a reseller). In addition, we also process personal data because the processing is necessary for our legitimate interests to be able to fulfil our agreement with our client, for administrative purposes, to handle disputes, prepare reports, communicate with your employer and provide you with the services.

- Name
- Staff number
- User Identifier (a file to associate your identity across various platforms)
- Date and time of reserved workplace (if you use workplace management)
- Miles driven (if you use kilometre registration)

- Address of the start and end-point of the trip

We also process these relevant categories of personal data for the non-mobility users who only file expense claims.

We store this data for a maximum of 7 years from the date of collection.

3.7 Apple and/or Google Pay users

XXImo offers device tokenization to its customers, via the digital wallets of Apple and Google. Both make use Visa Tokenization Service (VTS). Enrolling with these services can be done in two ways:

A. Push provisioning

Push provisioning is when you as a cardholder use the Milo app to initiate the enrolment process for Apple Pay or Google Pay. The following data elements are exchanged with the wallet app in this scenario:

- Account number
- CVV2 value
- The expiration date of the card
- Country of the cardholder
- Wallet Account ID (Internal ID associated with the cardholder)

B. Manual provisioning

Manual Provisioning is when the enrolment is done via the Apple Pay or Google Pay app. In this case, when the details are entered by you in the wallet app(s), XXImo receives an enrolment request from VISA (containing PAN, CVV2, and expiration date). This enrolment request is a form of account verification and contains extra data elements specific for fraud scoring on enrolment requests, including:

- IMEI
- OS type (Android/iOS)
- Device country (where the device resides at the moment)
- Device serial number
- Device time zone
- Bluetooth MAC address
- User account age (number of days the account for this user exists on the phone)
- Wallet account age (number of days ago the wallet for this user was created on the phone)
- Days since the last activity
- Number of transactions on this account in the past 12 months
- Days since the last account change on this device
- Number of suspended cards on the account
- Country code of the wallet
- Number of active tokens
- Number of devices with active tokens for this account
- Number of active tokens on all devices
- Device language
- Device telephone number
- Device name (as given by the user)
- Cardholder address (as stored on account)
- Cardholder name (as stored on account)

- IP address
- Device location, lat./long. up to 4 digits precision
- Hashed email address

No specific information is shared about the transactions by XXImo with Apple Pay or Google Pay. While Apple and Google do capture additional information on your purchases, they do not share the same with XXImo. You as a user agree to this capturing of information when you enrol into Apple Pay or Google Pay.

Further, while XXImo shares monthly reports with Apple on usage and fraud, and summarises fraud figures on a quarterly basis with Google, these do not contain any personally identifiable information.

3.8 YOR24 Platform

If you are a user of the YOR24 platform we process the categories of personal data described below. We obtain this data from your employer or reseller and enrich it further.

User data:

- Email
- Full name
- Address
- Phone number
- Employer name
- Staff number
- Function and department
- Budget type
- Preferred Language
- Leaving date
- Starting date
- Function

Pay Group Mobility Package Declarations:

Are connected to your user information through the user identifier.

- Transaction ID
- Date and time of transaction (creation time and actual travel date)
- Distance travelled
- Locations of transaction (start and end-points)
- Account number
- Type of transaction
- Method of transaction
- Transaction category
- Device number
- Price of transaction
- Source of transaction

Devices:

Are connected to your user information through the user identifier.

- Device ID
- Account number
- Device number

- Type of device
- Device category
- Device token
- Connection information (To see if the connection still works and when it last succeeded)
- Device created by
- Date of device:
 - First ride
 - Alteration
 - Deletion date
 - Blocked at

We store this data for a maximum of 7 years from the date of collection.

3.9 Newsletters

A. Newsletter for the users of our services

If you are a user of our services, with your consent, we process the personal data listed below to send you the newsletters, and to monitor the effectiveness of our newsletters.

- Name
- Language
- Country
- Email address
- The device on which the Milo app is installed (if you use the Milo app)
- Whether and if yes tokens are activated
- Whether any transactions were made with Google and/or Apple Pay in the last 24 hours
- Whether the e-mail has been opened

We process this personal data until you unsubscribe from the newsletter. You can unsubscribe by using the 'unsubscribe' button at the bottom of each newsletter. Your e-mail address and the newsletter content are shared with our mail provider based in the United States. We have signed a processing agreement and standard contractual clauses approved by the European Commission with this party. The mail provider may therefore only process the data in line with our instructions.

B. Newsletter for our customers and contacts of our customers

If you are a customer of ours or are acting as our customer's contact person, with your consent, we process the personal data listed below to send you the customer newsletters and to monitor the effectiveness of our newsletters.

- Name
- Language
- Country
- Email address
- Whether the e-mail has been opened

We process this personal data until you unsubscribe from the newsletter. You can unsubscribe by using the unsubscribe button at the bottom of each newsletter. Your e-mail address and newsletter content are shared with our mail provider based in the United States. We have signed a processing agreement and standard contractual clauses approved by the European Commission with this party. The mail provider may therefore only process the data in line with our instructions.

C. Communication with the users of our services

When you use our services, we may send you communications to guide you through the process of onboarding for specific products and services. These communications are intended to help you use our services effectively and to keep you informed of important information related to your account.

To facilitate these communications, we process the following categories of personal data:

- Contact details
 - Full first name
 - Last name
 - Place of birth
 - Place of residence
 - Email address
 - Telephone number
 - Employer
- Identification data
 - Customer number
 - Date of birth
 - Bank account number
 - Nationality
- Account information
 - Application link
 - Discount code
 - Interests
 - Language
 - Country
 - Card number
 - Account status
 - Account mail settings
 - Provisioning dates
- Financial data
 - Outstanding balance
 - VGC-PS relationship number
- Technical information
 - OS installation
 - Wallet(s)
 - Country.
- Incentive-related data

This data is collected and processed based on our legitimate interests to provide you with relevant information and to facilitate your use of our services. We ensure that your data is kept secure and is not used for any purposes other than the aforementioned communications and services. You have the right to opt out of this processing, however, this may restrict our ability to communicate with you or guide you through our services in specific circumstances.

We store this data for a maximum of 6 months from the date of collection.

3.10 Events

If you wish to attend or participate in one of our events, we will process your name and email address to be able to invite you to the event and to get in touch with you about the event. This is necessary for our legitimate interests, to have you participate in the event.

We also process who your employer is, your job title, and the company size of your employer. We process this data to form an overview of the visitors joining our events, so we can adapt and improve our events accordingly. This is our legitimate interest, for which the data processing is necessary.

We receive the personal data described above from you and keep it in our records for up to 1 year from the date of the event. Any additional information that may have been shared with us including dietary requirements, etc. is deleted right after the event. If you agree to be captured at the event, we will be storing the pictures, based on your consent, for no longer than 1 year from the date of the event. If you wish to withdraw your consent for the same, you can reach out to us at privacy@xximo.com.

3.11 Contact XXImo

If you contact us, we will process the personal data contained in the correspondence, the processing of which is necessary to respond to your queries or requests, and the phone number if you call us, your e-mail address if you send us an e-mail, and/or your Facebook username if you contact us via Facebook Messenger.

Our legal basis is that such processing is necessary for us to pursue our legitimate interests in being able to contact you and serves your legitimate interest by allowing you to contact us. We store this data for the duration of the contract with the customer and 2 years after the relationship between the customer and XXImo ceases to exist. Should there be any high-risk data involved, we reserve the right to store this information in line with the periods of limitation as discussed under Section 9.

If you contact our customer desk, we also record the conversations and store them for training and quality purposes for a period of 6 months. We do not process the same beyond the aforementioned purposes. Additionally, we also collaborate with HMS, our first-line service desk partner. They also record the calls for training and quality purposes and do not process them beyond the same. These recordings are stored by them for 3 months.

3.12 Persons covered by the XXImo screening

If you are a director, a shareholder, a beneficial owner or a politically prominent person of our customer, or are employed by our client, you may be subject to mandatory XXImo screening as required by the law. In this case, we carry out customer due diligence. This is only done for the relations (customers, UBOs, authorised representatives, and cardholders) of XXImo Financial Services B.V. We keep the data for 5 years after the end of the contract with the customer. To conduct the same, we process the following categories of personal data:

- Full first name(s) and surname
- Contact information
- Date of birth
- Place of birth
- Nationality
- Gender
- Place of residence
- Country of residence
- Identity document
- Copy of the document
- Company name
- Company official street address
- Company statutory seat
- Company Chamber of Commerce number
- Company VAT number
- Company business activities

- Company share structure
- Company website
- Source of Wealth
- Industry you work in
- UBO qualification
- Politically exposed person (PEP) qualification
- Authorised representative qualification

We may request additional documents to verify this data, including a copy of your identification documents. We only do this if there is a legitimate reason to do so, or if we cannot verify the data by other means. In that case, we will store a copy of the shared documents. Those documents may contain more information than described above, such as your home address or your percentage of shares.

To communicate with you regarding the screening, we also processed your e-mail address.

If you are a politically prominent person, we also process the origin of your assets and resources and process your political office. Your political office may also involve special personal data. We may process this data under Dutch financial regulations such as Wft, and Wwft.

Based on the personal data described above, you and the client are assigned to a risk class. This classification is done automatically. The moment the system classifies you in a higher risk class, a human check will take place to assess to which risk class you belong.

If you are on a sanctions or terrorism list, we will report this to the competent supervisory authority. We do not inform you about this.

3.13 Corporate clients and contacts of our corporate clients

A. Creditworthiness tests

We conduct tests to assess the creditworthiness of our customers. We use the Dun & Bradstreet credit report to conduct this test. For this purpose, we process the personal data (retrieved from the Dun & Bradstreet credit report) below from our customer(s) and its employee(s). Our legal basis for the processing of personal data is that it is necessary for our legitimate interests to be able to assess the customer's creditworthiness.

- Company name
- Business address
- Phone number
- How long the company has been in existence
- Number of employees
- Corporate structure and subsidiaries
- VAT number
- Credit score (retrieved from Dun & Bradstreet)
- Capital (retrieved from Dun & Bradstreet)
- Financial statements for the past five years
- Whether you are (or have been) in arrears
- Where your entity is registered
- Power of attorney of director
- LinkedIn profile

We store this data for a maximum of 2 years from the date the relationship between XXImo and the customer ceases to exist.

B. Contract

The personal data provided in this section is required to request a demo, consultancy, or a contract from XXImo. XXImo needs to be able to communicate with the contact person of the (intended) customer and therefore has a legitimate interest in processing that contact person's data. The processing is also necessary for drawing up and signing a contract. We store the contract (and the personal data covered therein) for the duration of the contract, and up to 5 years after the relationship between the customer and XXImo ceases to exist in line with the administrative and contractual obligations. XXImo reserves the right to retain this for longer should there be legal obligations, in line with Section 9. The categories of personal data processed for these purposes are mentioned below:

- Name
- Gender
- Date of birth
- Phone number
- Email address
- Employer
- Function (not in case of application through OMW2)
- Chamber of Commerce number
- Branch address
- Business bank details
- Signature
- Business address

C. Additional information provided

Not providing the above personal data or objecting to its processing may affect your company or employer's ability to enter into a contract with us request a demo, or seek consultancy.

D. Processing the data of the contacts in our business relations

If you work for a business relation, such as a supplier or a business customer, and you are the contact person of one of our entities, that entity processes the personal data below because it is necessary to pursue the legitimate interest of communicating with businesses and for executing the contracts concluded with your employer. The personal data will be kept for 2 years after the contract with your employer has come to an end / you cease your employment with the employer or until the relationship between the business relations and XXImo ceases. The data is provided by you or one of your colleagues.

- Name
- Employer
- Function
- Phone number
- Email address

3.14 Applicants

If you apply for a position at a XXImo entity, that entity will process the personal data listed below for up to 4 weeks after the completion of the application or up to 1 year if you wish to be considered for future opportunities. The legal basis for processing the data is the entity's legitimate interest in processing and concluding your application.

- Name
- Email address
- Phone number
- CV (including any photo)

- Motivation letter
- Communications regarding the applications
- Information to be found about you on the internet (through an internet check)
- Certificate of good conduct (if considered reasonable for the intended position)
- An assessment regarding your capabilities (if considered reasonable for the intended position)
- Input from referees you provide (if you permit us to approach them)

4. Processors

We may use so-called data processors to process your personal data on our behalf. We conclude processing agreements with these processors so that they only process your personal data for the purposes determined by us.

We use the following types of processors:

- Hosting providers;
- Card providers;
- Developers and suppliers of software;
- Vendors of client record and identification software;
- Transaction monitoring software;
- Customer administration software;
- Customer contact centre;
- Mailing software providers;
- Security solution providers;
- Analytics software providers.

If you provide additional data to these processors yourself outside our service, we are not responsible for this. It is wise to inform yourself well about the processor and its company before providing additional personal data.

5. Sharing your personal data

We may also share your personal data with others. Above, we have described with whom and under what circumstances we share your personal data with others. In addition, we may also process and share your personal data with third parties if:

- Necessary to comply with our legal obligations;
- Necessary to comply with legal requests from authorities;
- Required to respond to any legal claims;
- Necessary to protect the rights, property or safety of us, our users, our employees, or the public;
- It is required to protect ourselves or our users from fraudulent, abusive, inappropriate, or unlawful use of our services.

We will notify you as soon as possible if a government agency makes a request that relates to your personal data unless we are prohibited from doing so by law.

We may also disclose, share, or transfer your personal data when we transfer part of our business. Examples include (negotiating) a merger, selling business units, and/or obtaining loans. Naturally, we try to minimise the impact for you by only transferring personal data when necessary and anonymising it where possible.

6. Protecting your personal data

Protecting your personal data is of utmost importance to us. We have therefore taken appropriate technical and organisational security measures to protect your personal data. These measures include, but are not limited to the following:

- We only use trusted database providers to store data that have taken adequate physical and electronic measures to minimise the risk of unauthorised access, loss or misuse of personal data.
- We use TLS (Transport Layer Security) technology to encrypt sensitive information or personal data, such as account passwords.
- We make backups of personal data.
- Sensitive information is stored in an encrypted form.
- Vulnerabilities in the software are fixed as soon as reasonably possible.

Please note that we cannot guarantee absolute security when transmitting personal data over the Internet or storing personal data. We recommend that you consider this before sharing personal data.

7. Links to third-party sites

Our websites and apps may contain links to other websites and services. These third-party websites and services may collect and store information about you. If you provide your personal data to third parties, we are not involved. We have no control over these sites or the activities of the third parties. In that case, the third party's privacy policy will apply. We are not responsible for the content of these parties' privacy statements or their handling of personal data. We encourage you to read their privacy and security practices and statements before providing personal information to them.

8. Your rights as a data subject

As a data subject, you have certain rights concerning your personal data. The rights we describe below are not absolute. We will consider whether we can reasonably meet your requests. If we cannot comply with your request because your request is manifestly unfounded or excessive or if your request would compromise the privacy of others, we may refuse to comply with it. If we refuse a request, we will sufficiently inform you of the reasons for refusal.

Right to access

You have the right to request which personal data we process about you. You can also ask us to provide insight into the grounds for processing, relevant categories of personal data, the (categories of) recipients of personal data, the retention period, the source of the data and whether or not we use automated decision-making.

You can also request a copy of your personal data that we process. Do you want additional copies? If so, we may charge a reasonable fee for these.

Right to rectification

If the personal data of you processed by us is incorrect or incomplete, you may request us to amend or supplement the personal data.

If we grant your request, we will also, as far as reasonably possible, inform the parties to whom we provide information.

Right to be forgotten/ Right to erasure

Do you no longer want us to process certain personal data about you? Then you can reach out to us requesting the deletion of certain (or all) categories of personal data concerning you. Whether or not we undertake deletion of the data depends on the grounds of processing. The data that we process based on a legal obligation or in the performance of the agreement can only be deleted if it is no longer needed. If we process data based on our legitimate interest, we will only delete data if your interest outweighs ours; the same will be assessed by us. If we process data based on consent, we will only delete data if you withdraw your consent. Have we accidentally processed data or does a specific law require us to delete data? Then we will delete the data. If the data is necessary for the settlement of legal proceedings or a (legal)

dispute, we will only delete the personal data after the conclusion of the proceedings or dispute(s).

If we grant your request, we will, as far as reasonably possible, inform the parties to whom we provide information.

Right to restrict processing

If we process data based on a legitimate interest, you can object to the processing. If you dispute the accuracy of personal data processed by us, if you believe that we have processed your personal data unlawfully, if we no longer need the data, or if you have objected to the processing: you can request us to restrict the processing of your personal data. If we restrict the processing of your personal data at your request, we may still use that data for the resolution of legal proceedings or a (legal) dispute.

Right to data portability

At your request, we may transfer to you or another party designated by you, the data that we process in performance of the agreement, or based on your consent. You may make such a request at reasonable intervals.

Automated individual decision-making

We do not make decisions solely based on automated processing that produce legal effects on you or otherwise significantly affect you.

Right to the withdrawal of consent

If you have provided your consent to us for processing certain personal data, you are free to withdraw the consent at any given time. We shall cease the processing of the data if your consent is the sole legitimate basis we are using to process the specified categories of personal data. For more information, please refer to the relevant processing purposes above.

Exercising your rights

You can send a request for access, correction, deletion, or data transfer of your personal data, or a request to withdraw your consent or object to the processing of your personal data to the mail address listed below in the contact details. We will then ensure that the request reaches the appropriate entity.

To prevent abuse, we may ask you to adequately identify yourself when making a written request for inspection, rectification, or deletion.

We aim to process your request, complaint or objection within one month. If it is not possible to make a decision within one month, we will inform you of the reasons for the delay and when the decision is expected to be made (no later than 3 months from receipt of the request).

Data Protection Authority

Do you have a complaint about our processing of your personal data? If so, please contact us. We will be happy to help you. If we cannot work it out together, you also have the right to lodge a complaint with the Dutch Data Protection Authority. To do so, please contact the relevant authorities at <https://autoriteitpersoonsgegevens.nl>.

9. Period of Limitation

XXImo will retain the personal data highlighted in this privacy statement in line with the retention periods discussed herein. Further, XXImo is required to store the contract data for 5 years from the date on which the relationship between the customer and XXImo ceases to exist to meet the administrative and contractual obligations. Further, XXImo reserves the right to retain the personal data elements highlighted in this statement beyond the set retention

timelines for up to 5 years to meet the contractual obligations, and beyond that to meet the administrative, and legal obligations, i.e. for preparing, pressing, or defending legal claims.

10. Contact

If you have any questions, comments, or concerns about this privacy statement and/or our data processing, or have any data subject requests or reports of data breaches, please contact our Privacy Officer by sending an email to privacy@xximo.com.

If you have any additional concerns, you can also reach out to our external Data Protection Officer (DPO) at dewi.harkink@osborneclarke.com. You must not send data subject requests or data breach reports to our DPO since XXIMO cannot then guarantee a timely response per the stipulated timelines due to the secret nature of the DPO mailbox.