

Annex 1 TPML Privacy Policy

TPML Privacy Policy

Version 3.0

This policy explains when and why we collect personal information about you, how we use it, the conditions under which we may disclose it to others and how we keep it secure.

TPML is committed to safeguarding the privacy of your information. By “your data”, “your personal data”, and “your information” we mean any personal data about you which you or third parties provide to us.

We may change this Policy from time to time so please check this page regularly to ensure that you’re happy with any changes.

Who are we?

Transact Payments Malta Limited (“TPML”, “we”, “our” or “us”) is the issuer of your card and is an independent Data Controller for the personal data which you provide to us to enable us to issue and maintain the card services. TPML is an e-money institution, authorised and regulated by the Malta Financial Services Authority. Our registered office address is Vault 14, Level 2, Valletta Waterfront, Floriana, FRN 1914, Malta and our registered company number is C91879.

Orenda Financial Services Limited is the Program Manager for your card program and is an independent Data Controller for any personal data which you provide which is related to facilitating the management of the card program. Orenda Financial Services Limited is incorporated and registered in England and Wales with registered office at St. Martins House 1, Gresham Street, London EC2V 7BX and company registration number 12404984.

Potje Technologie B.V. administers and provides the Card associated with the Program. Potje Technologie B.V. is incorporated in the Netherlands with company registration number 84112905 and registered office address at Badhuiskade 11, s-Gravenhage, 2586.

How do we collect your personal data?

We collect information from you when you apply online or via a mobile application for a payments card which is issued by us. We also collect information when you use your card to make transactions. We may also process information from Program Manager, other third-party payment partners and service providers. We also obtain

information from third parties (such as fraud prevention agencies) who may check your personal data against any information listed on an Electoral Register and/or other databases. When we process your personal data, we rely on legal bases in accordance with data protection law and this privacy policy. For more information see: ***On what legal basis do we process your personal data?***

On what legal basis do we process your personal data?

Contract

Your provision of your personal data and our processing of that data is necessary for each of us to carry out our obligations under the contract (known as the Cardholder Agreement or Cardholder Terms & Conditions or similar) which we enter into when you sign up for our payment services. At times, the processing may be necessary so that we can take certain steps, or at your request, prior to entering into that contract, such as verifying your details or eligibility for the payment services. If you fail to provide the personal data which we request, we cannot enter into a contract to provide payment services to you or will take steps to terminate any contract which we have entered into with you.

Legal/Regulatory

We may also process your personal data to comply with our legal or regulatory obligations.

Legitimate Interests

We, or a third party, may have a legitimate interest to process your personal data, for example:

- To analyse and improve the security of our business;
- To anonymise personal data and subsequently use anonymized information.

What type of personal data is collected from you?

When you apply for a card, we, or our partners or service providers, collect the following information from you: full name, physical address, email address, mobile phone number, phone number, date of birth, place of birth, nationality, gender, login details, IP address, identity and address verification documents.

When you use your card to make transactions, we store that transactional and financial information. This includes the date, amount, currency, card number, card name, account balances and name of the merchant, creditor or supplier (for example a supermarket or retailer). We also collect information relating to the payments which are made to/from your account. If we are required by law to process additional

personal data (for example, if we suspect that there may be fraud related to the use of your card or the payment services linked to it), we will also process that extra personal data.

How is your personal data used?

We use your personal data to:

- set up your account, including processing your application for a card, creating your account, verifying your identity and printing your card.
- maintain and administer your account, including processing your financial payments, processing the correspondence between us, monitoring your account for fraud and providing a secure internet environment for the transmission of our services.
- comply with our regulatory requirements, including anti-money laundering obligations.
- improve our services, including creating anonymous data from your personal data for analytical use, including for the purposes of training, testing and system development.

Who do we share your information with?

When we use third party service partners, we have a contract in place that requires them to keep your information secure and confidential.

We may receive and pass your information to the following categories of entity:

- identity verification agencies to undertake required verification, regulatory and fraud prevention checks;
- information security services organisations, web application hosting providers, mail support providers, network backup service providers and software/platform developers;
- document destruction providers;
- Mastercard, Visa, digital payment service partners or any third party providers involved in processing the financial transactions that you make;
- anyone to whom we lawfully transfer or may transfer our rights and duties under this agreement;
- any third party as a result of any restructure, sale or acquisition of TPML or any associated entity, provided that any recipient uses your information for the same purposes as it was originally supplied to us and/or used by us.
- regulatory and law enforcement authorities, whether they are outside or inside of the European Economic Area (EEA), where the law requires us to do so.

Sending personal data overseas

To deliver services to you, it is sometimes necessary for us to share your personal information outside the European Economic Area (EEA), e.g.:

- with service providers located outside the EEA;
- if you are based outside the EEA;
- where there is an international dimension to the services we are providing to you.

These transfers are subject to special rules under European and Malta data protection law.

These non-EEA countries do not have the same data protection laws as Malta and EEA. We will, however, ensure the transfer complies with data protection law and all personal information will be secure. We will send your data to countries where the European Commission has made an adequacy decision, meaning that it has ruled that the legislative framework in the country provides an adequate level of data protection for your personal information. You can find out more about this [here](#).

Where we send your data to a country where the European Commission has not made an adequacy decision, our standard practice is to use standard data protection contract clauses that have been approved by the European Commission. To obtain a copy of those clauses, please go to the [European Commission's website](#).

If you would like further information, please contact our Data Protection Officer on the details below.

How long do we store your personal data?

We will store your information for a period of five years after our business relationship ends in order that we can comply with our obligations under applicable legislation such as anti-money laundering and anti-fraud regulations. If any applicable legislation or changes to this require us to retain your data for a longer or shorter period of time, we shall retain it for that period. We will not retain your data for longer than is necessary.

Your rights regarding your personal data?

You have certain rights regarding the personal data which we process:

- you may request a copy of some or all of it;
- you may ask us to rectify any data which we hold which you believe to be inaccurate;
- you may ask us to erase your personal data (where applicable);
- you may ask us to restrict the processing of your personal data;
- you may object to the processing of your personal data (where applicable); and
- you may ask for the right to data portability.

If you would like us to carry out any of the above, please email your request to the Data Protection Officer at dpo@transactpay.com.

How is your information protected?

We recognise the importance of protecting and managing your personal data. Any personal data we process will be treated with appropriate care and security.

These are some of the security measures we have in place:

- we use a variety of physical and technical measures to keep your personal data safe;
- we have detailed information and security policies to ensure the confidentiality, integrity, and availability of information;
- your data is stored securely on computer systems with control over access on a limited basis;
- our staff receives data protection and information security training on a regular basis;
- we use encryption to protect data at rest and anonymization where applicable;
- we have adequate security controls to protect our IT infrastructure and staff computers including but not limited to Identity and Access Management, Firewalls, VPN, Antivirus, Advanced Email Threat Protection and more; and
- we conduct regular audits such as PCI-DSS to ensure we are following adequate security controls to protect your data.

While we take all reasonable steps to ensure that your personal data will be kept secure from unauthorised access, we cannot guarantee it will be secure during transmission by you to the applicable mobile app, website or other services over the

internet. However, once we receive your information, we make appropriate efforts to ensure its security on our systems.

Complaints

We hope that our Data Protection Officer can resolve any query or concern you may raise about our use of your personal information.

The [General Data Protection Regulation](#) also gives you right to lodge a complaint with a supervisory authority, in particular in the European Union (or European Economic Area) state where you work, normally live or where any alleged infringement of data protection laws occurred. The supervisory authority in Malta is the Office of the Information and Data Protection Commissioner. Their contact details are as follows:

IDPC,
Floor 2, Airways House, Triq il-Kbira, Tas-Sliema, SLM1549, Malta.
(+356) 23287100 / info@idpc.org.mt

Other websites

Our website may contain links to other websites. This privacy policy applies only to our website, so we encourage you to read the privacy statements on the other websites you visit. We cannot be responsible for the privacy policies and practices of other sites even if you access them using links from our website.

Changes to our Privacy Policy

We keep our Privacy Policy under review and we regularly update it to keep up with business demands and privacy regulation. We will inform you about any such changes. This Privacy Policy was last updated on 23rd December 2025.

How to contact us

If you have any questions about our Privacy Policy or the personal information which we hold about you or, please send an email to our Data Protection Officer at dpo@transactpay.com.