

Mynt AB

INTEGRITY & PRIVACY POLICY

Effective date: 2021-06-01

General

Mynt's integrity & privacy policy describes how Mynt AB, org. no. 559100-8874 (hereinafter "Mynt", "we" or "us"), processes personal data collected through websites, partners and other channels. It also describes which cookies are used on the website to improve the user experience and enable us to provide our service.

Mynt is a financial institution registered with the Swedish Financial Supervisory Authority and mainly conducts corporate finance operations.

Mynt values your privacy and personal information and works with appropriate technical and organizational security measures to ensure that your privacy is not violated and that your personal information is treated fairly, legally and transparently. Our privacy policy states why and how we process your personal data, that it is done correctly, and that we do not store more of it or longer than necessary. Of course, we process your personal data in accordance with current EU data protection legislation.

This privacy policy applies to you who are a customer of ours, work for a company that is a customer of ours or has been in contact with us.

Digital channels

Digital channels include our websites and social media such as mynt.se, mynt.com and certain other services that we provide online, as well as HTML-formatted e-mails that we send to you (collectively referred to as our "Digital channels").

Your consent

We need your consent to be able to deliver our service. If you do not want us to process your personal data, you cannot use the website or any of our services.

How we handle personal data

Why do we process your personal data?

To be able to deliver our services

We process your personal data in order to be able to deliver and administer the service you or the company you work for have shown interest in according to our business agreement or have ordered from us. We need to be able to establish your identity and make a fair credit assessment of your business. We may also share your personal information with the third party who has mediated the contact. We also use personal information to be able to respond to inquiries that you make to our customer service. Examples of personal data that we use for this purpose are contact information (such as name, title, professional role, telephone number and address) as well as order and payment history (such as purchase and transaction history and payment information).

For our customers: Our legal basis is fulfilment of agreements.

For those who are employed by a company that is a customer of ours: Our legal basis is balancing of interests, as we assess that our interest in fulfilling our agreement with your company outweighs your interest in the protection of your personal data.

To improve the user experience

We use your personal information to be able to provide you with a better and more user-friendly service. We think it is important that it is easy for you to use our service. This mainly applies to your experience of registration, application, signing of an agreement and login. Personal data is also processed to be able to adapt the display of content in digital channels, to the device you use and provide you with an improved user experience.

Our legal basis is balancing of interests, as we assess that our interest in providing you with a better and more user-friendly service outweighs your interest in the protection of your personal data.

To be able to present relevant offers and recommendations

We want to be able to provide you with relevant recommendations and offers based on your company's conditions, for example by sending you newsletters. Please note that you always have the right to demand that we stop using your personal information for direct marketing.

For you who are a customer with us: Our legal basis is balance of interests, as we assess that our interest in providing you with relevant recommendations and offers outweighs your interest in the protection of your personal data (for marketing via e-mail, SMS, MMS and others automatic systems if certain legal requirements are met).

For those who are not customers with us: Our legal basis is consent.

To analyze trends and further develop our products and our offer

We use personal data to better understand market trends and thus further develop and improve our digital channels, our products, services and our offering.

Our legal basis is balance of interests, as we assess that our interest in analyzing trends and further developing our products and our offer outweighs your interest in the protection of your personal data.

To prevent, limit and investigate abuse of our channels

We may need information about user behaviour, activities and technical data in order to prevent, limit and investigate any violations and misuse of our channels such as false personal data, spamming, embezzlement or attempts to log in with another user's personal data and other behaviours that are prohibited by law.

Our legal basis is a balance of interests, as we assess that our interest in preventing, limiting and investigating the misuse of our channels outweighs your interest in the protection of your personal data.

Administration in connection with company acquisitions, restructuring of Mynt, etc.

If an outside party wishes to acquire Mynt or our customer database, Mynt will disclose your and others' personal information to the acquiring company. In that case, that company will continue to use your personal information for the same purposes as those we have stated in this privacy policy if you do not receive other information in connection with the transfer.

Our legal basis is balancing of interests, as we assess that our interest in enabling an acquisition process outweighs your interest in the protection of your personal data. However, this presupposes that the acquiring company conducts similar activities as Mynt.

To fulfil our legal obligations and to prevent and prosecute crimes

We use your personal information to fulfil our legal obligations, e.g. according to the requirements of the Accounting Act and the Money Laundering Act.

Our legal basis is a legal obligation.

We will also disclose information about you if we receive a request from prosecutors or police.

Our legal basis is in the public interest, for the purpose of preventing or prosecuting crime.

How do we collect personal data?

We collect personal data in different ways:

Via digital channels: We collect personal information via our digital channels when you, for example, sign up for a newsletter, receive product offers, want to be contacted, download a material, send information to us via email or start an application for a business loan or register for another of our services.

Offline: We may collect personal information via other non-digital channels if, for example, you visit us at an event, during a telephone call or if you otherwise meet one of our sales representatives or contact customer service.

Via other sources: In order to constantly improve our service and provide you with relevant marketing and offers, we may collect information about you through other partners such as a public database, marketing partners who have your consent or social media.

We may receive information from people who act on your behalf, for example with the support of a power of attorney or as a representative of a company in which you are involved (eg as an owner or board member). We can also get information from social media and advertising platforms and analytics providers.

We may combine information we receive from you with information about you that we receive from third parties, where this is permitted by law. For example, we may combine information we have collected offline with information we collect online, to the extent covered by the purpose of the transaction or your consent. In the same way, we can also combine information we receive from a third party with information we already have.

How do we use personal data?

Personal data is used as described in this privacy policy and in accordance with what is required by applicable law.

Examples of primary uses:

- to establish your identity
- to conduct credit assessments of your business
- to answer your wishes or questions
- to improve our websites, our services and our tools, e.g. credit rating models.
- to administer our website and our internal operations.
- for security purposes. Where permitted by law, we may use your information to protect our business, our customers and our websites.
- to fulfil our legal obligations, e.g. at a money laundering check.
- for information and marketing purposes. For example, we may send you information about new services and special offers (with your consent if you are not already a customer of ours).

Automatic decision making

Note that we use credit data for automated decision making in credit assessment. This means that an automated credit assessment will be made of your and your company's financial circumstances to see if you will be able to repay the financing we give you. The automated decision is made on the basis of information about payment remarks, assets and liabilities. If the credit rating indicates that you will not be able to repay the financing, your request may be denied. If you have views on the decision made, you have the right to contact us. We will then review the information behind the decision and any additional information you have given us. The review will take place by a person who has the authority to change the decision if it turns out that the decision has been made on incorrect grounds.

How do we secure personal data?

We use standard security measures and carry out ongoing organizational, technical and administrative measures to protect personal data within our organization. While we take reasonable steps to protect your personal information, you should be aware that no security procedures or protocols are guaranteed to be 100 percent secure from intrusion or hacking. Therefore, there is always a certain risk assumed by sharing personal information online. All transmission of data to us via digital channels takes place at your own risk. We encourage you to be careful when using the internet. This includes not sharing your passwords. If you have reason to believe that your contact with us is secure, contact us immediately (see "Contact" below).

How long do we store personal data?

We retain your personal information and other information only for the time necessary to fulfil the purposes described in this privacy policy and other requirements set by law. When your personal information is no longer relevant for the purposes for which it was collected, we will delete or de-identify it. As an example, we

store personal data related to the Accounting Act for seven years, calculated from the end of the calendar year in which the financial year to which the information belonged ended, in accordance with law, and related to money laundering for at least five years, calculated from the time the relevant measures or the transactions were performed or the business relationship ended. According to current statute of limitations, certain information, such as receivables, saved for up to 10 years.

How do we share personal information?

Where the law allows, we may share information with third parties with whom we do business. We may also share your personal information with the police or prosecutor upon such request.

In cases where a third party has mediated the contact between you and us, we report information about our dealings with such third party. It can e.g. refer to the size and number of credits granted, how the repayment of the credits is handled and other information provided in connection with you taking out a loan and during the term of the loan.

We may share information with a successor to all or part of our business. For example, if part of our business or assets are sold, we may include user information as part of this transaction. See more about this under "Why do we process your personal data?" above.

Which cookies do we use and why?

We use cookies on our website to improve the user experience and to be able to deliver our service. Cookies are small text files that are saved in your computer's browser when you visit a website. On return visits, these can be downloaded from the browser for different types of applications. This website uses cookies for the following applications:

- Analysis of the website (Google cookie)

Examples of information that we may collect via these cookies:

- Demographic information.
- Gender, age, language settings and which browser and Olympics are used
- Information about your mobile device
- Pages visited on our website
- Geographical information
- Aggregated information, we can collect and analyze information about users over time such as:
 - Time of visit
 - Which pages were visited and for how long
 - Referring websites, applications or services

We may have a third party who collects information in this way, e.g. Google tracking.

How to disable cookies

If you do not want cookies to be saved in your browser, it is possible to completely or partially block cookies. It is also possible to delete cookies when they have already been saved in your browser. Both actions are available via the settings in your browser and exactly how you do it depends on which browser you are using. You can use the browser's help function or read more at <http://www.aboutcookies.org/> for more detailed information on how to do this in the browser you are using.

As a visitor to a website, you should be aware that certain parts of the website may not work if you choose not to save or delete cookies.

Read more at <http://www.aboutcookies.org/> for more detailed information about which cookies are, how they work, what they are used for and what you should do as a visitor if you want to refuse or revoke your consent to the use of cookies.

Your rights

You have several rights that you have the right to use. We will follow your request as soon as possible. If you wish to object to the processing, access to, correct, delete or restrict the use or disclosure of personal data about you that has been collected and stored by Mynt's, revoke your consent or exercise any other right under applicable data protection law, please notify us at info@mynt.se, so that we can investigate and

respond to your request in accordance with applicable law. You can also request a copy of your personal data (data portability). Please note that revocation of consent does not affect the legality of the processing due to consent before it is revoked.

You can also revoke your consent to marketing communications at any time. You do this by sending an email to info@mynt.se, or by clicking on the "unsubscribe" or "opt-out" link at the bottom of our emails sent for marketing purposes.

If you have any concerns about our privacy policy, we appreciate if you contact us directly so we can answer all your questions.

Third Party Websites

Our digital channels may allow you to link to other websites on the Internet via direct links or through applications such as "share" or "like" buttons, and other websites may also contain links to our digital channels. The content of such other websites is not governed by this privacy policy, but the privacy policy set forth by these third party websites.

Updates

We update these terms on an ongoing basis. The date at the top of the page indicates when this policy was last revised. Any changes to this policy will take effect when we publish the revised policy on our website mynt.se. Significant changes to our policy will be notified 10 days before they take effect.

Contact Us

Your privacy is important to us. If you have any questions, concerns or complaints about how we collect and use your personal information, you are welcome to contact us via email at info@mynt.se. Or by letter:

Mynt AB, Vasagatan 28, 111 20 Stockholm

For card users: Transact Payments Limited privacy policy

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.

TPL 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 Limited ("TPL", "we", "our" or "us") is the issuer of your card and is the Data Controller for the personal data which you provide to us in relation to the card only. TPL is not the Data Controller in relation to any use of your personal data to send marketing or promotional material to you. TPL is an e-money institution, authorized and regulated by the Gibraltar Financial Services Commission. Our registered office address is 6.20 World Trade Center, 6 Bayside Road, Gibraltar, GX11 1AA and our registered company number is 108217.

Enfuce is the Program Manager of your card and is a Data Processor of the personal data which you provide to us in relation to the card.

How do we collect your personal data?

We collect information from you when you apply for a payments card which is issued by us and when you use your card to make transactions. 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.

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, 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 analyze and improve the security of our business;
- To anonymize personal data and subsequently use anonymized information.

What type of personal data is collected from you?

When you apply for, and use, a card, we, or our partners on our behalf, collect the following information from you: Full name, personal ID number, email address, Social Security Number (SSN), phone number, account balances, transactional and cryptographic data, technical data, location, IP address, and card data.

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. We also collect information relating to the payments which are made to/from your account.

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 and verifying your identity.
- 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?

We pass your information to our third party service providers, agents, subcontractors, program managers and other associated organizations for the purposes of completing tasks, managing your account and providing services to you on our behalf, as detailed above. When we use third party service providers, we have a contract in place that requires them to keep your information secure and confidential.

We pass your information to the following categories of entity:

- companies and organizations that assist us in processing transactions you make (including but not limited to payment processing service providers) and in providing services that you have requested;
- companies and organizations that run and manage the card program;
- identity verification agencies to undertake required verification, regulatory and fraud prevention checks;
- information security services organizations, web application hosting providers, mail support providers, network backup service providers and software/platform developers;
- document destruction providers;
- 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 TPL 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 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 Gibraltar data protection law.

These non-EEA countries do not have the same data protection laws as Gibraltar 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 at least six 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 requires us to retain your data for a longer 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.
- You may ask us to restrict the processing of your personal data.
- You may object to the processing of your personal data.
- You may ask for the right to data portability.
- If you would like us to carry out any of the above, please email the Data Protection Officer at DPO@transactpaymentsltd.com.

How is your information protected?

We implement security policies and technical measures in order to secure your personal data and take steps to protect it from unauthorized access, use or disclosure.

While we strive to protect your personal information, we cannot guarantee the security of any information you transmit to us, and you do so at your own risk. Once we receive your information, we make our best effort to ensure its security on our systems. Where we have given (or where you have chosen) a password which enables you to access certain parts of our websites, you are responsible for keeping this password confidential. We ask you not to share your password with anyone.

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 Gibraltar is the Gibraltar Regulatory Authority. Their contact details are as follows:

Gibraltar Regulatory Authority,
2nd floor, Eurotowers 4, 1 Europort Road, Gibraltar.
(+350) 20074636/(+350) 20072166 info@gra.gi

The supervisory authority in Sweden is:
Datainspektionen
5th Floor
Box 8114
104 20 Stockholm
Tel. +46 8 657 6186
Fax +46 8 652 8652
Email: datainspektionen@datainspektionen.se

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 12th October 2020.

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@transactpaymentsltd.com.