



# Paywerk AS Privacy Notice

We respect your right to privacy and are committed to protecting your personal data. This privacy notice contains important information about how and why we use your personal data and your rights as a data subject.

---

## 1. Who is responsible for your personal data?

Paywerk AS, with the registry code 16218310 and registered address at Niine 11, Tallinn, Estonia („**Paywerk**“, „**we**“ or „**our**“) provides payment services and is the data controller responsible for your personal data under General Data Protection Regulation (EU)

2016/679 („**GDPR**“) and other applicable data protection legislation. Under personal data we mean any information which can be used to identify you (e.g. the combination of your name and address).

Paywerk also provides an online payment platform to merchants and financiers, where consumers can choose between different flexible payment options. This means when you make a purchase with a merchant and receive financing from your preferred financier via Paywerk's platform, the

merchant and the financier will be responsible for processing of your personal data within their respective services. Therefore, you should read the privacy notices of the merchant and financier carefully as these will also apply to and explain how your personal data is used.

In addition to consumers, this notice describes how Paywerk processes personal data of data subjects representing merchants, financiers, and other partners.

---

You can contact us any time via the contact details available at our website or at [dpo@paywerk.co](mailto:dpo@paywerk.co).

---

## 2. What kind of personal data do we collect?

We collect personal data directly from you when you are:

- registering an account with us (personal details and contact data);
- filling in forms or interacting with our websites (personal data input in the contact forms, device data);
- using our services (data regarding your payments);

We also collect data from third parties, such as:

- merchants (data about your shopping session);
- external registries (reports from credit bureaus and anti-fraud services).

---

## 3. What is our lawful basis for using your personal data?

- We use your data to enter into a contract with you and provide you with our services during the term of our contract. This includes customer on-boarding, concluding, and performing the contract(s) between us, customer relationship management and customer support. Without the contractually required data we will not be able to provide our services.
- We use your personal data to comply with our legal obligations under data protection, payment services, anti-money laundering and counter-terrorist financing and other applicable legislation. Without the legally required data we will not be able to provide our services.
- We use your data for our legitimate business interests. This means we have a legitimate business interest in using your data which has been assessed and balanced with your privacy rights in each case. These include prevention of financial fraud, security of our IT-systems and intra-group transfers.
- We may also use your data if you consent, e.g. to receiving marketing offers from us or our carefully selected partners. Your consent is voluntary and asked separately for each purpose, e.g. by asking you to tick a box. You may always withdraw your consent, e.g. in our website or by following the opt-out instructions included in each marketing message, but please note this does not affect the lawfulness of the processing during the validity of the consent.

### 3. How do we protect your personal data?

We respect your privacy and make sure your personal data is processed securely. We understand the world around us is constantly changing and we are analyzing the risks and mitigations to your personal data on an on-going basis.

We apply several technical and organizational security measures to protect your data from unauthorised or accidental access, loss or modification. Your data is secured both in transit by using encrypted communication protocols and at rest by using ISO/IEC 27001

certified data centres. We have internal policies in place, and we train our personnel in data protection and information security to make sure following our policies are complied with in our daily operations.

---

### 5. How do we use cookies and other tracking technologies?

To improve and customize our services, we use cookies and other tracking technologies ("cookies") in our websites. Cookies are small files that are stored on your device and help us to recognize you. When you interact with our websites, you will be provided relevant

information about cookies and how to accept or decline them. You can also manage or delete cookies by changing your browser settings, but please note in this case some of the functionalities of our websites may not work correctly.

We mainly use 3 types of different cookies for the following purposes:

- Essential cookies are used to provide access to different parts of our websites and therefore cannot be disabled. Essential cookies are generally stored on your device in response to your actions on the website, e.g. filling in forms or managing cookie preferences.
  - Analytical cookies are used to measure and improve the customer experience on our websites by counting unique visitors, source of the visits and understanding how users interact with our websites.
  - Marketing cookies are used to see what pages and links you visit and thereby customize information about our services and provide more relevant ads to you. We may share information collected via marketing cookies with social media providers.
-

## 6. Your rights

If you have any questions or wish to exercise any of your rights below, please contact us by e-mail at [dpo@paywerk.co](mailto:dpo@paywerk.co)

Please note we always need to identify you to make sure your request is legitimate, and your personal data is safe from fraudulent attempts. We will reply at the latest within 30 calendar days from your request and free of charge, except when your request is unfounded or excessive.

Under GDPR, you have the rights to

- 1 **obtain information** about how we process your personal data, provided in this privacy notice and by answering your questions;
  - 2 **access your data** by receiving an electronic copy thereof;
  - 3 have your incomplete or inaccurate **data rectified**;
  - 4 **withdraw your consents**, where we use your data based on your consent, e.g. sending marketing offers;
  - 5 **delete your data**. Please note in some cases we cannot comply with your request. As a financial services provider, we need to store certain data for a period required by law;
  - 6 **restrict the processing of your data** in certain cases, e.g. when we investigate if the data is accurate or you have objected to using your data;
  - 7 **object to us processing your data**, e.g. you can always object to using your data for marketing purposes. You can also object to any processing based on our legitimate interest, but please note if we believe our business reason overrides your rights, we cannot comply with your request;
  - 8 **transfer your data to another company**. In certain cases, we can provide your data processed by us in a structured, commonly used and machine readable format;
  - 9 in case of automated decisions with legal effect, to **object to the automated decision** by expressing your point of view and obtaining human intervention;
  - 10 **submit a complaint** to the relevant data protection authority. In Estonia, the data protection authority is Andmekaitse Inspektsioon ([www.aki.ee](http://www.aki.ee)), for other EU countries the contact details of the respective authorities can be found [here](#).
-

## 7. How do we profile and make automated decisions about you?

In some cases, we may make a partially or fully automated decision that has legal effect on you. This means we use technology that takes into account information, including your personal data, necessary to predict our contractual risks and ensure our services are secure. If you are not approved based on the automated decision, you will not have access to our services. Such decisions include:

- approving or declining your application for our financial services based on personal data provided by you, our internal information and data collected from merchants and/or credit bureaus
- determining the risk of financial fraud and/or money laundering, based on personal data provided by you and collected from third parties, such as fraud prevention agencies.

We apply mechanisms to make sure our profiling and automated decision making are relevant by regularly checking our decisioning algorithms and based on a random selection, a number of the automated decisions.

You always have a right to object to an automated decision by contacting us at [dpo@paywerk.co](mailto:dpo@paywerk.co). Based on your objection, our employee will manually review the decision considering any additional information and viewpoints you may have submitted.

---

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

Where and to the extent we disclose your personal data, we always enter into a data processing agreement to ensure the recipient uses your personal data securely and only to the extent required for a specific service. When you use our services, your personal data is disclosed to the following categories of recipients:

- Our group companies for administrative and corporate purposes;
- Merchants for purchasing your product;
- Financiers selected by Paywerk to enable offering you financing;
- Credit bureaus for risk scoring;
- Our suppliers and sub-contractors such as:
  - IT and data hosting suppliers;
  - payment services partners and payment networks (VISA, Mastercard);

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

- identity verification service partners;
- fraud prevention agencies;
- debt collection service providers in case of outstanding debts;
- legal and financial advisers;
- social media platforms in case you log-in or contact us via social media platforms.
- In certain cases, we are obliged by law to disclose your data to regulatory authorities (e.g. the Financial Supervisory Authority, tax or other investigative authorities) only to the extent of the defined legal obligation(s).

## 9. How long do we keep your data?

We retain your data for the minimal necessary period after which your data is depersonalized. We determine the retention periods of your data based on:

- the purposes of processing outlined in this privacy notice;
- applicable legislation, such as accounting, taxation, payment and anti-money laundering laws;
- potential or on-going legal disputes between us, in which case we may keep your data longer based on our legitimate interest.

---

## 10. Where do we store your data?

Your data will be stored within the European Economic Area. Our suppliers may transfer your data outside the EEA for limited purposes, but in these cases, we always make sure the suppliers implement appropriate security measures and safeguards with non-EEA data recipients, in particular signing standard protection clauses approved by the European Commission.

---

## 11. Updates

We may update this privacy notice from time to time. The latest version of the privacy notice is always available on our website.