

## Pliant Oy Privacy Policy

This privacy policy applies to the issuance of credit cards and, where applicable, the provision of the credit card processing account by Pliant Oy.

The following describes the scope and purpose of collection and use of personal data by Pliant Oy and informs about the rights to which data subjects are entitled under data protection law. Definitions of the terms used (e.g. "personal data" or "processing") can be found under Art. 4 of the General Data Protection Regulation ("GDPR"). Pliant Oy takes your data protection very seriously and treats your personal data confidentially and in accordance with the statutory provisions. Accordingly, your personal data will not be sold and will only be passed on to third parties if there is a legal basis or with your consent.

### 1. Who are we?

Pliant Oy ("Pliant Oy", "we", "our" or "us") is the issuer of your credit card and, where applicable, additionally the provider of your credit card processing account and data controller in terms of GDPR for the personal data which you provide to us in relation to these services:

Pliant Oy  
Pohjoisesplanadi 19  
00100 Helsinki  
Finland  
email: [info@getpliant.com](mailto:info@getpliant.com)

Pliant Oy is an e-money institution, authorised and regulated by the Finnish Financial Supervisory Authority (FIN-FSA).

Our parent company, Pliant GmbH ("**Pliant Germany**"), is the operator of the Pliant platform and is the data controller for any personal data which you provide which is not related to the card or account. Pliant Germany is incorporated and registered in Germany with its registered office at Prenzlauer Allee 242-247, 10405 Berlin, Germany. For the use of the website [getpliant.com](https://getpliant.com) and the Pliant app, please read Pliant Germany's privacy policies for the [website](#) and the Pliant app which apply additionally.

If a credit card processing account is not provided by Pliant, but by a partner bank (e.g. Varengold Bank AG), please read the partner bank's privacy policy which applies additionally in this case.

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

We collect information from you when you apply online or via a mobile application for a credit card issued by us and, where applicable, for a credit card processing account provided by us. We also collect information when you use your card to make transactions and, where applicable, when such transactions are settled via the credit card processing account provided by us. We may also process information from Pliant Germany, other third-party payment partners and service providers. We also obtain information from publicly available sources (commercial register) or third parties (such as credit agencies, fraud prevention agencies) who may check your personal data against any information listed on public registers 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 (see section: On what legal basis do we process your personal data?).

### **3. 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:

- Name,
- Contact details (such as physical address, email address, phone number),
- Identity verification data and documents (such as date and place of birth, nationality, address, ID card/passport copy, video identification data, tax number) of legal representatives and ultimate beneficial owners,
- Card user identification data, where applicable (such as name, date of birth, nationality, address, ID card/passport copy)
- Login details, IP address.

When you use your card to make transactions, we store that transactional and financial information such as

- date, amount, currency
- card number, card name
- account balances
- name of the merchant, creditor or supplier (for example a supermarket or retailer).

If you use a credit card processing account provided by us, we may additionally process and store

- Information about your financial information (such as credit data, scoring/rating data, source of funds), including information from credit and fraud prevention agencies,
- Date, amount, currency, reason, recipient of payments made from/to your account,
- Account balances,
- Credit limits.

If you use the Company Reimbursement Service, we additionally process and store

- the details of the personal payment card (including first and last name, card number, card type, expiration date, verification number (CVC or CVV)) a card user has provided

as well as the amount to be collected in connection with the use of this service to reimburse your company for expenses deemed personal or outside the scope of your company's policies.

Note regarding the source of data: For the purposes of complying with anti-money laundering and tax obligations, we may process identity verification data and documents (e.g., name, date and place of birth, nationality, address, ID card/passport copy, video identification data, tax number) of legal representatives and ultimate beneficial owners of your company that we have obtained from our partner bank Varengold Bank AG, other banking partners and/or identity verification agencies.

#### **4. 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, printing, shipping and delivering your card;
- maintain and administer your account, including processing your financial payments, monitoring your account for fraud/misuse and providing a secure internet environment for the transmission of our services;
- where applicable, maintain and administer your credit card processing account, including processing your financial payments, monitoring your account for fraud/misuse and all other activities required in connection with operation and management of a loan and financial services institution;
- process the correspondence between us, including when you or any of your related persons exercise your or their rights under data protection law and make requests;
- comply with legal and /or regulatory requirements, including know-your-customer and anti-money laundering obligations;
- For establishment and defence of legal rights;
- improve our services, including creating anonymous data from your personal data for analytical use, including for the purposes of training, testing and system development.

#### **5. On what legal basis do we process your personal data?**

##### **Contract fulfilment, Art. 6 (1)(b) GDPR**

The provision of your personal data and our processing of that data is necessary to carry out our obligations under the agreement (the corporate owned funds credit card Terms and Conditions of Use or the Pliant Payment Services Terms and Conditions, as applicable) 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 need to take steps to terminate any contract which we have entered into with you.

## **Legal obligations, Art. 6 (1)(c) GDPR**

We may also process your personal data to comply with legal and/or regulatory obligations. This includes performing 'Know Your Customer' (KYC) checks, complying with Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) regulations, and preventing financial crime. Additionally, we use this data to adhere to tax laws, regulatory reporting requirements, and international sanction screening to ensure the security and integrity of our financial services.

## **Legitimate interests, Art. 6 (1)(f) GDPR**

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

- To answer requests addressed to us;
- Where applicable, to identify credit and/or default risks;
- To prevent and/or investigate criminal acts such as fraud;
- For marketing purposes, unless you have objected to the use of your data for this purpose or revoked a marketing consent once given;
- To cede open claims to a new creditor (cessionary) by contractual agreement;
- To secure our claims arising in connection with the business relationship;
- To entrust debt collection agencies with the collection of open claims;
- To assert legal claims and defence in legal disputes;
- To ensure IT security and IT operations of Pliant Oy and Pliant GmbH;
- To anonymise personal data and subsequently use anonymized information, e.g. for product development.

## **Consent**

Insofar as you have given us your consent to the processing of personal data for specific purposes, the legality of this processing is based on your consent. This granted consent can be revoked at any time with future effect, e.g. by writing an email to [privacy@getpliant.com](mailto:privacy@getpliant.com).

## **6. Who do we share your information with?**

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

- Identity verification agencies, fraud prevention agencies and credit agencies to undertake required verification, regulatory and fraud prevention checks;
- Card schemes (currently Visa), financing partners, banking providers (currently Banking Circle and/or Varengold), digital payment service partners or any third party providers involved in processing the financial transactions that you make;
- Cessionaries, in case we decide to cede an open claim to a third party by contractual agreement;
- Insurances or guarantors, if any, to secure our claims arising in connection with the business relationship;
- Debt collection agencies in case of default of payments;
- Our legal and other professional advisors, including our auditors;

- Regulatory, law enforcement and/or other public authorities, where the law requires us to do so.

Furthermore, we pass on your data to service providers who support us in the operation of our websites and app and the associated processes as part of data processing on behalf in accordance with Art. 28 GDPR (data processors). Our data processors are strictly bound by instructions and contractually obligated to us accordingly. These are service providers in the following categories:

- affiliated companies who act as outsourcing providers on our behalf
- information security services organisations
- web application hosting providers
- mail support providers
- network backup service providers
- software/platform developers
- document destruction providers
- whistleblowing service providers.

Data processors process the data exclusively on our instructions and are obliged to comply with the applicable data protection regulations. All data processors have been carefully selected and will only have access to your data to the extent and for the period necessary to provide the services.

The servers of some of the data processors we use are located in the USA and other countries outside the European Union/European Economic Area. Companies in these countries are subject to data protection laws that do not generally protect personal data to the same extent as they do in the Member States of the European Union/European Economic Area. There is currently no decision by the EU Commission that third countries generally offer an adequate level of protection. If your data is processed in a country that does not have a recognised high level of data protection such as the European Union/European Economic Area, we ensure that the level of data protection is secured as far as possible by means of contractual regulations (e.g. the standard data protection clauses provided by the EU Commission for the processing of personal data in third countries with data recipients in third countries in accordance with Art. 46 (2)(c) GDPR) or other recognised instruments.

When you become a Pliant customer, we collect general company information including information about your legal representatives and contact persons (such as their business contact data, their role in the company and, where applicable, their right of representation) for the purposes of contract initiation, contract fulfillment, and customer communication. In this respect, we and Pliant GmbH process the data as so-called joint controllers within the meaning of Art. 26 GDPR and have concluded agreements as to which of us fulfills which data protection obligations; we will provide you with the essential content upon request. Further information on the data processed by Pliant GmbH can be found in Pliant GmbH's privacy notices. If you have any questions regarding the assertion of data subject rights, you can contact both us and Pliant GmbH (e.g. via email to [support@getpliant.com](mailto:support@getpliant.com)).

## **7. How long do we store your personal data?**

Unless we have already informed you in detail about the retention period, we delete personal data when they are no longer required for the aforementioned processing purposes and no legal retention obligations prevent deletion.

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.

## **8. Processing of special category of personal data (health data)**

When we provide payment services in the context of insurance products, card users may use the credit card to settle events covered under insurance policy, including but not limited to medical treatment, medical supplies or other insured events that may reveal health-related information. In addition to information such as the date, amount, currency and card number, as well as the name of the card user and account balances, which is processed in connection with the use of credit cards, special categories of personal data within the meaning of Art. 9 of the GDPR may be processed in this context. This may include information relating to medical services or supplies, as well as healthcare provider details.

Pliant processes such health-related personal data solely for the purposes of facilitating payment services, reimbursements and claims handling in the insurance context. The processing of health-related personal data concerning card users is based on the explicit consent of the data subject in accordance with Art. 9 (2)(a) GDPR. Consent is obtained when the card user either applies for or is issued with the card in the insurance context, and/or when the card user actively submits receipts, invoices or other supporting documents via the Pliant platform for reimbursement or claims handling purposes. Consent may be withdrawn at any time with future effect, e.g. by writing an email to [privacy@getpliant.com](mailto:privacy@getpliant.com). The withdrawal of consent does not affect the lawfulness of processing carried out on the basis of consent prior to its withdrawal.

In relation to Pliant's direct customers (such as insurance companies), the processing of information necessary to facilitate and settle payments for insured events is carried out for the performance of the contract between Pliant and the respective customer in accordance with Article 6(1)(b) GDPR.

## **9. Click to Pay (CTP)**

Where we make available Card Scheme Click-to-Pay ("CTP) functionality, personal data is processed to enable users to use Click-to-Pay for eligible purchases, to complete payment

transactions, to provide authentication (including device-based authentication such as Passkeys, where used), to apply card-related benefits, and to support customer service and dispute handling.

In this context, Pliant may process the following categories of personal data: card users identification data (such as name and contact details), card details (processed in accordance with card scheme security standards), transaction data (including merchant name, date and amount), device identifiers (where used for authentication purposes), and authentication data that remains stored locally on the card user's device.

For the processing activities described above, Pliant acts as a joint controller together with the relevant card scheme, as set out in the agreement (the Pliant Payment Services Terms and Conditions). Pliant responsibilities include the collection of card user enrollment data and its transmission to the relevant card scheme. Card schemes (such as Visa and Mastercard) and participating merchants may process CTP-related data under their own terms and privacy notices. Certain elements of the CPT functionality may also be provided by third-party service providers; in such cases, only the necessary data to enable the functionality is shared.

The processing of personal data necessary to provide and manage the CTP functionality is carried out on the basis of performance of the contract (Art. 6 (1)(b) GDPR). Where the use of CTP requires additional consent or permissions by card users ((for example, for specific authentication methods or value-added services offered by card schemes or third parties), such processing is subject to separate consent mechanisms or the respective third party's lawful basis.

Participation in the Click-to-Pay functionality is voluntary. Card users may opt out of CTP at any time, without affecting their ability to use the card for other payment methods.

Further information on the processing of personal data by the card schemes can be found in the [Visa Global Privacy Notice](#) and [Mastercard Click to Pay Privacy Notice](#).

## **10. Your rights regarding your personal data?**

When processing your personal data, GDPR grants you certain rights as a data subject:

### Right of access (Article 15 GDPR)

You have the right to request confirmation as to whether personal data concerning you are being processed; if this is the case, you have the right to be informed about these personal data and to receive the information listed in detail in Art. 15 GDPR.

### Right of rectification (Art. 16 GDPR)

You have the right to request the correction of any inaccurate personal data relating to you and, where applicable, the completion of any incomplete data without delay.

#### Right to erasure (Art. 17 GDPR)

You have the right to request that personal data concerning you be deleted without delay, provided that one of the reasons listed in detail in Art. 17 GDPR applies.

#### Right to the restriction of processing (Art. 18 GDPR)

You have the right to request the restriction of processing if one of the conditions listed in Art. 18 GDPR applies, for example, if you have objected to the processing, for the duration of the review by the controller.

#### Right to data portability (Art. GDPR)

In certain cases, which are listed in detail in Art. 20 GDPR, you have the right to receive the personal data concerning you in a structured, common and machine-readable format, or to request the transfer of this data to a third party.

#### Right of objection (Art. 21 GDPR)

***If data are collected on the basis of Art. 6(1)(f) GDPR (data processing for the protection of legitimate interests), or on the basis of Art. 6(1)(e) GDPR (data processing for the protection of public interests, or for the exercise of official authority), you have the right to object to the processing at any time on grounds relating to your particular situation. We will then no longer process the personal data unless there are proven compelling legitimate grounds for the processing which override your interests, rights and freedoms, or the processing serves the assertion, exercise or defence of legal claims.***

#### Right of appeal to a supervisory authority (Art. 77 GDPR)

In accordance with Art. 77 GDPR, you have the right to lodge a complaint with a supervisory authority if you are of the opinion that the processing of data concerning you violates data protection regulations. The right of appeal may in particular be exercised before a supervisory authority in the Member State of your habitual residence, place of work, or place of the alleged infringement.

## **11. 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 [privacy@getpliant.com](mailto:privacy@getpliant.com).