The Legal Details

Legal bases for processing

In many of the countries where we operate, data protection law requires us to process personal data only where we have an approved basis under the law. You have the right to understand what our legal bases are, so we explain them here. We use the following bases, depending on the activity we undertake:

1. Necessary for the performance of a contract
Most of the data we collect and the purposes we use it for are **necessary for us to provide our services.**

2. Necessary to comply with law and regulation
Some of the activities we undertake are necessary to comply with our **legal and other obligations** as a payment provider, for example:

- Anti-money laundering and sanctions compliance
- Activities connected with claims and litigation

To comply with our anti-money laundering and customer due diligence obligations, we must collect information on merchant criminal history. Where we do so, we comply with the requirements of law for collecting this category of data. In the UK, we collect this data under the "substantial public interest conditions" of Schedule 1 of the UK Data Protection Act 2018.

3. Necessary to meet our legitimate interests and not outweighed by your rights
We use personal data as **necessary to meet our legitimate business interests**. When we do, we make sure we understand and work to minimise its privacy impact. For example, we limit the data to what is necessary, control access to the data, and where we can, aggregate or de-identify the data.
Some examples of the data processing activities we undertake in our legitimate interests are:

- Preventing fraud and unauthorised use
- Preventing payment failures and speeding up payment processing times
- Marketing our services to prospective merchants
- Communicating news and industry events to our current and prospective merchants and partners
- Hosting and participating in events
- Developing and improving our products and services

What is legitimate interest? Under GDPR Article 6(1)(f), companies have the ability to engage in activities without consent under a balancing test. Do we have a legitimate interest in engaging in the activity that is not outweighed by the interests or fundamental rights and freedoms of the data subject

4. In rare cases, with your specific and informed consent
We tell you in the service where you can make a choice or grant consent. When you grant consent, you may **withdraw it** at any time to stop any further processing.

Automatic decision-making

Technology helps us make automatic decisions based on the information we collect about you or a transaction. We routinely test our software to improve the accuracy of these decisions and to prevent unintended bias. These decisions can have effects for you, such as:

- Preventing access to our services, if we determine there is a high likelihood that it would violate our regulatory requirements - for example, if the identification you provide does not match public records, identity verification or credit reference information.
- Cancelling transactions, if we determine there is a high likelihood that there are insufficient funds to cover it or that it is fraudulent - for example, because the payment is made from a location that does not match our records.
- Cancelling the service, if we determine that it is being used in violation of our terms - for example, if any of the activities you conduct appear on our list of restricted activities.

If you believe a decision has been made in error, please contact us.

Your rights and choices

You may have rights under privacy and data protection law. Depending on where you live, these include the right to **ask GoCardless for a copy** of your personal data, to **correct**, **delete** or **restrict** processing of it, and to **obtain personal data in a format you can share with a new provider**. You may have the right to **object** to processing. These rights may be limited in some situations – for example, where we can demonstrate that we have a legal requirement to process your data.

You can contact our privacy team to ask a question about our privacy practices or exercise your rights. If you have unresolved concerns, you have the **right to complain** to a data protection authority or other regulator where you live or work, or where you believe a breach may have occurred.

How is personal data shared?

- We share personal data with the **merchants, payers and financial institutions involved in a transaction**.
- GoCardless works with partners **who integrate our payment services into their applications**. When you make a payment through a partner integration, or when you set up a GoCardless account with one of our partners, your personal data will be shared with the partner to provide the integrated services.
- We share merchant data with **GoCardless companies** located in countries where we offer the GoCardless payment services, who use it to provide and market our services in those countries, governed by this privacy notice.
- If ownership or control of all or part of our business or assets changes, we may transfer personal data to the **new owner**. If the owner will use the data

for purposes other than those disclosed here, they will take the steps required by law to ensure such purposes remain lawful.

- We work with **service providers** who have access to personal data when they provide us with services, like technical infrastructure, web and app development, and marketing, analytics and survey tools. We impose strict restrictions on how service providers store, use and share data on our behalf. We also work with companies who provide identity verification, background screening, due diligence, consulting and other regulatory services for us.
- In exceptional circumstances, we share personal data with **government agencies and other third parties** if we believe it is reasonably necessary to comply with law, regulation, legal process or governmental request; to enforce our agreements, policies and terms; to protect the security of our services; to protect GoCardless and our merchants, payers or the public from harm or illegal activities; or to respond to an emergency.

International transfers

GoCardless' services are offered from our United Kingdom headquarters and from GoCardless offices in France, Germany, Australia and the United States. Our services are available to merchants in a number of countries around the world. If you use our services to pay a merchant in another country, personal data will be transferred as necessary to complete this transaction.

Personal data may also be stored and accessed by service providers located in other countries. For EU individuals, it's important to note that some of our service providers are located in the United States or other countries that do not provide the same standard of data protection as the EU. Wherever we transfer data, we enter into contracts or seek other ways to ensure service providers treat data as required by law in the country where it was collected.

How long do we keep personal data?

GoCardless keeps personal data for as long as necessary to provide our services and process payments for our merchants. We also keep personal data for other legitimate business purposes, such as complying with our legal obligations, resolving disputes, preventing fraud, and enforcing our agreements. Because these needs can vary for different data types used for different purposes, retention times will also vary. Here are some of the factors we have considered to set retention times:

- How long do we need the personal data to develop, maintain and improve our services, keep our systems secure, execute chargebacks, prevent fraudulent transactions, and store appropriate business and financial records.
- Have you asked us to stop using your data or withdrawn your consent? Where we can delete the data, we will process it for only a short period after this to meet your request. If needed, we will also keep a record of your request so that we can make sure it is respected in the future.
- Are we subject to a legal, regulatory or contractual obligation to keep the data? For example, we're required to keep transaction data and other information that helps us carry out required checks, for periods of time that vary according to the underlying payments scheme. We may also need to comply with government orders to preserve data relevant to an investigation or retain data for the purposes of litigation.