

GoCardless Global Privacy Notice

Updated 14 May 2018

You can find the [previous version here](#)

Contents

Who is GoCardless?.....	1
What personal data do we collect?.....	2
How do we use personal data?	3
How is personal data shared?	5
International transfers	6
Your rights and choices	6
How long do we keep personal data?	6

Who is GoCardless?

GoCardless provides services that help merchants process payments for their goods or services. The controller for the personal data involved when you use GoCardless, visit our website or communicate with us, or transact with a merchant using our payment services, is:

GoCardless Ltd.
Sutton Yard, 65 Goswell Road
London, EC1V 7EN
United Kingdom

[Contact our Data Protection Officer or exercise your data protection rights \(including your right to object\)](#)

Merchants who use our payment services are also data controllers. If you have questions about how a merchant handles your personal data, or if you wish to exercise your rights for the personal data they hold, please contact them directly.

What personal data do we collect?

Visitors

We collect personal data when you use our website, make an inquiry or communicate with us.

- **Information about your use of our online content and emails**, such as how you came to our website, which pages you visit, how long you remain on a page or view a video, and whether you opened an email or clicked a link. To collect this data, we use [cookies and other tracking technologies](#).
- **Information provided when you communicate with us by phone, email, webform or chat**, including records of your contact, your country and language, your email address or other contact information, and other information about the reasons for the communication.
- **Business information that tells us more about our prospective merchants and partners**, from companies like Dun & Bradstreet, Mint and other data enrichment sources, and from public sources like LinkedIn or Twitter.
- **Marketing preferences**, such as whether you have agreed to receive marketing information or newsletters about our services or whether you have opted out, and the types of services that may interest you.

Merchants & Partners

We collect personal data when you enquire about, set up, administer and use a GoCardless account. This may include information about your company's employees, directors, trustees or beneficial owners.

- **Identification information**, such as name, email address, phone number, birthdate, government-issued identification (for example, a passport or driver's license), and account username and password.
- **Financial information**, such as sort code, bank account number and account holder name and address.
- **Transaction information**, such as the names of transacting parties, a transaction description, payment amounts, billing and shipping information, and the devices and payment methods used to complete the transactions.
- **Device and connection information**, such as the type of device you use to access our services, operating system and version, device identifiers, network information, log-in records, IP address and location derived from it.
- **Merchant verification information**, from agencies who provide identity verification or credit references (for example, Onfido, LexisNexis or Creditsafe), from financial institutions (such as our banking partners Royal Bank of Scotland PLC and Barclays Bank PLC), from social media such as LinkedIn or from other public sources. We confirm your identity and may check reports

of your credit and employment history and businesses with which you are connected. Where applicable, we may access your criminal history, presence on sanctions lists or in adverse media searches, and links to politically exposed persons.

Payers

We collect personal data when you set up and make or have a payment collected using our services.

- **Identification and contact information**, such as your name, home address, and email address. Where required by law or financial institutions, we also collect a government identifier.
- **Financial information**, such as your bank account number, sort code, account holder name, and other information you provide to us or give us consent to access directly from your bank. Using tools on our website, like Truelayer, you can choose whether to let us access personal data directly from your bank account so that we can verify that you are the owner of the account. This includes your balance and personal details registered to your bank account.
- **Transaction information**, such as the names of the transacting parties, a description of the transactions, the payment amounts, billing and shipping information, and the devices and payment methods used to complete the transactions.
- **Device and connection information**, such as the type of device you use to access our services, operating system and version, device identifiers, network information, IP address and location derived from it.
- **Payer verification information**. If our banking partner or our own fraud alerts flag a potentially fraudulent payment or account, we will use identity verification and screening agencies like Onfido or Lexis Nexis and other publicly available data to confirm the payer's identity and clear the alert or stop the payment or chargeback.

How do we use personal data?

Using personal data to provide our services

We use personal data where it is necessary to provide the services you request.

- **To provide payment services**, we use the identification, contact and financial information of merchants and payers. We use transaction information to deliver key features of the services, such as displaying transaction history.
- We use personal data **to communicate with you**, like sending payment notifications, alerting you to changes in the service, or providing **customer support**.
- We use personal data to **prevent fraudulent or unauthorised use of our services**. We verify the identity of merchants and in some cases payers, evaluate the authenticity of payments,

and may block transactions we believe to be fraudulent or violate our terms. To do this, we rely on software that makes **automatic decisions**:

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 significant 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](#).

Using personal data for our legitimate interests

We use personal data for 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.

- We use personal data to **develop and improve our products and services**. For example, we might use data to:
 - create or refine models for detecting unauthorised transactions and improving the speed at which transactions are processed
 - analyse how people engage with our website and services so that we can develop new products or features.
- Where we determine that a payment is likely to clear, by using personal data to **analyse the likelihood that payers have sufficient funds**, we may advance payments to merchants and partners to process transactions more quickly.
- We use personal data to **promote our services**, communicate news and industry updates, and host or participate in events.
- Where we believe it is necessary to **protect our legal rights and interests** and the interests of others, we use personal data in connection with legal claims, compliance, regulatory and audit functions, and in connection with the acquisition, merger or sale of a business.

Using personal data where required by law and payment schemes

We use personal data to comply with the requirements of law and the payment schemes we operate under, and as required in other exceptional circumstances.

- We must **conduct due diligence on our merchants and where necessary, payers**, and prevent money laundering or other illegal activities. We verify the identities of prospective and current merchants and their employees and beneficial owners, and screen them for sanctions, politically exposed persons, **criminal activity** and adverse media. We conduct background checks where required by law.

To collect sensitive data like criminal activity, we rely on the "*substantial public interest conditions*" in data protection law (for example, Schedule 1 of the UK Data Protection Act 2018).

- Under **exceptional circumstances**, we may be required by law to provide personal data to law enforcement agencies, courts or others in connection with claims and other litigation.

How is personal data shared?

- We share personal data with **financial institutions and the merchants and payers in a transaction** to provide our payment services.
- 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 data with **GoCardless companies** 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. Personal data may also be stored and accessed by service providers located in other countries in the European Union. 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.

When we work with a service provider, we look for a legal mechanism that requires them to protect data to EU standards. For example, the service provider has signed on to the EU-US Privacy Shield, operates under EU-approved binding corporate rules, or is in a country the EU recognises as having adequate data protection laws. Where no other legal mechanism exists, we enact the EU-approved standard contractual data protection clauses in our contracts.

Our services are available 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.

Your rights and choices

Most of the data we collect and the purposes we use it for are necessary for us to operate and improve our services or comply with our obligations as a payment provider. 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. You can also ask us at any time not to send or to carry out profiling for direct marketing, or to stop using certain kinds of cookies.

You may have certain rights under data protection law. 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.

[Exercise your data protection rights](#)

If you have unresolved concerns, you have the **right to complain** to an EU data protection authority where you live or work, or where you believe a breach may have occurred.

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? We will process the data for only a short period after this to implement 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.