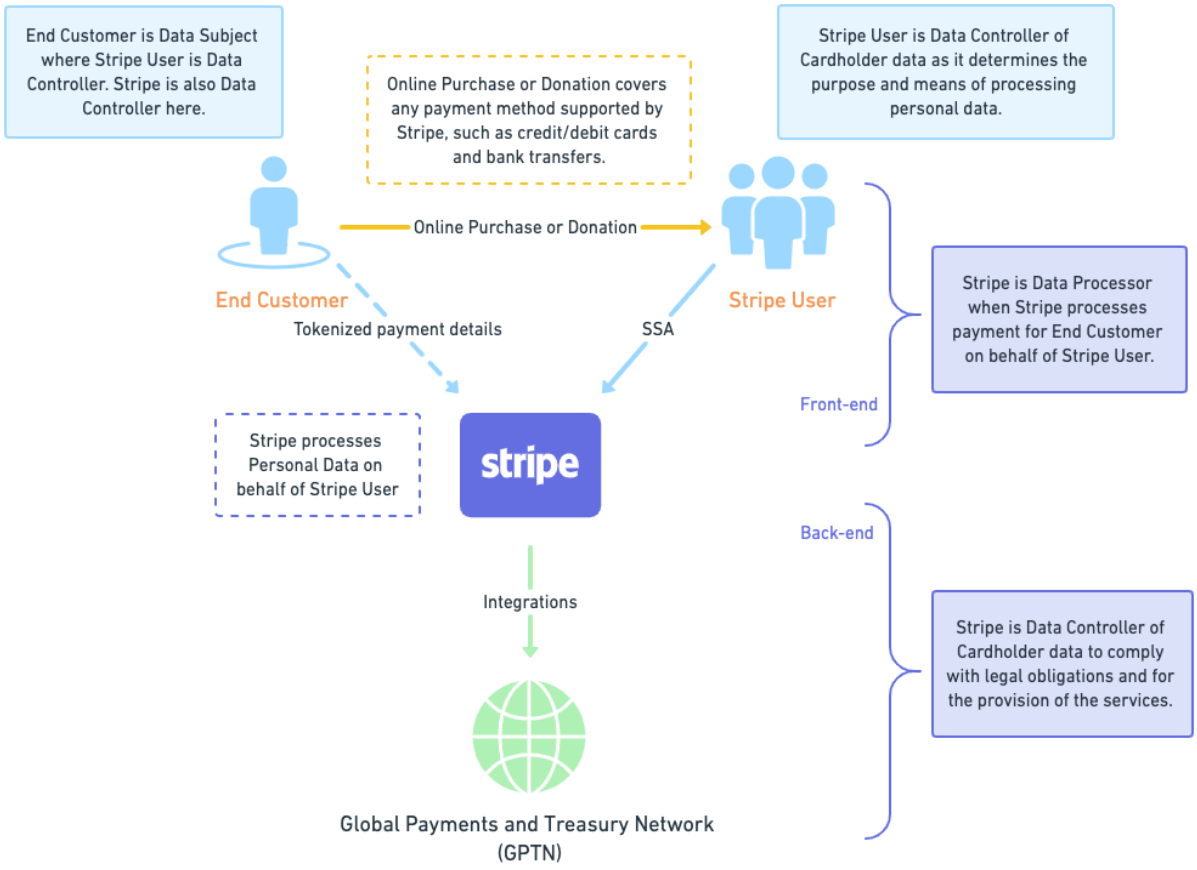
Stripe Privacy InfoPack

Overview

This document explains how Stripe processes your and your End Customers' data when you use Stripe's services. It also provides answers to most common questions on Stripe's privacy and security practices.

How data processing works

Here is a simplified overview of Stripe's payment processing flow, including a brief description of the data processing responsibilities involved.



For more information on online payments, see our guide Introduction to online payments.

Helpful Terms

Below is a list of terms that will help “you” navigate this InfoPack:

Term	Meaning	Example
Business User	Stripe provides services to entities (“Business Users”) who directly and indirectly provide us with “End Customer” personal data in connection with those Business Users’ own business and activities.	Stripe user or merchant Platform User Connect Accounts
End Customer	When you do business with, or otherwise transact with, a Business User (typically a merchant using Stripe Checkout, e.g., when you buy a pair of shoes from a merchant that uses Stripe for payment processing) but are not directly doing business with Stripe, we refer to you as an “End Customer.”	Individual using Identity Cardholder using Checkout
End User	When you directly use an End User Service (such as when you sign up for Link, or make a payment to Stripe Climate in your personal capacity), for your personal use, we refer to you as an “End User.”	User of Link with Stripe Personal contributor to Stripe Climate
Representative	When you are acting on behalf of an existing or potential Business User (e.g., you are a founder of a company, or administering an account for a merchant who is a Business User), we refer to you as a “Representative.”	Beneficial owner Shareholder, officer, director Account representative
Visitor	When you visit a Site without being logged into a Stripe account or otherwise communicate with Stripe, we refer to you as a “Visitor” (e.g., you send Stripe a message asking for more information because you are considering being a user of our products).	Stripe Sessions attendee Stripe Site visitor

Is Stripe a Data Controller or a Data Processor?

In general, the answer is both.

The “data controller” is the entity which determines the purposes and means of the data processing taking place. The “data processor” is an entity acting on behalf and under the instructions of a controller in processing personal data.

Our standard payment processing data flow, where Stripe Business Users (merchants) use Stripe’s technology to enable cardholders (End Customers) to pass card data directly to Stripe, is a PCI compliant way to process the card data without it ever touching Stripe Business Users’ servers. This allows Stripe to assume the relevant PCI compliance obligations directly.

Critically, the flow of the card data does not determine who is the controller and who is the processor. Rather, the “data controller” is the entity that determines the purpose and means of the data processing activity, and the “data processor” is the entity acting on behalf and under the instructions of the data controller in carrying out the data processing activity. The primary question is whether the activity takes place because Stripe was instructed to do so (Stripe is processor) or because Stripe chooses or is otherwise obligated to carry out the activity on its own (Stripe is controller).

Stripe is a **data controller** when it determines the purposes and means of the processing taking place. These data processing activities include (1) providing the Stripe products and services to Business Users and End Users, (2) monitoring, preventing and detecting fraudulent payment transactions and other fraudulent activity on the Stripe platform, (3) complying with legal or regulatory obligations applicable to the financial sector to which Stripe is subject (e.g. KYC requirements, payment reconciliations with financial partners, and anti-money laundering and sanctions screening), and (4) analysing, developing and improving Stripe’s products and services.

Stripe is a **data processor** where it is servicing the Stripe platform and facilitating payment transactions on behalf of and at the direction of a Stripe Business User. Our Business Users direct us to take payment from cardholders, i.e., whom to pay, how much to pay, when to pay, what currency to apply. Stripe does not determine who the End Customer will be, how much that End Customer should pay or when the payment should occur.

As a platform provider, we need to ensure consistency across our platform, and that includes consistency with respect to the commitments that we give about how we operate our platform. We contract with all of our Business Users (including some of the world’s largest companies) on this basis.

We note that for certain products, Stripe may act as an independent data controller (e.g., Stripe Capital), a data processor or both (e.g., Stripe Identity). For more information, please see the Privacy Center article for each specific product.

For more information on the controller / processor roles, see our Privacy Center here. Please see our Stripe legal bases tables to learn how and why we use personal data as a controller.

Helpful Resources

We have created some additional resources that provide additional information on Stripe's data protection and privacy practices:

- Stripe Privacy Policy here
- Stripe Privacy Center here
- Stripe Service Providers List here
- Stripe Cookie Policy here
- Stripe Cookie Settings Dashboard here

Frequently Asked Questions

Below answers are framed in the context of GDPR but are still applicable globally.

➔ Basics

Does Stripe have a Data Protection Officer (DPO)?

Stripe has an appointed Data Protection Officer (DPO), and they can be reached via email at dpo@stripe.com. Stripe also has a German DPO who can be contacted at the same address.

Does Stripe have dedicated persons/teams for privacy compliance?

Yes. Data security, data protection and compliance with all applicable privacy and data protection rules is at the heart of our business operations. We have a dedicated team within security engineering, privacy program managers, and a privacy-legal team to address Stripe's privacy compliance obligations.

➔ Information Collection from Individuals

What data elements are collected and processed about individuals?

Personal data is any information that relates to an identified or identifiable individual, and can also include information about how the individual engages with our Services (e.g., device information, IP address).

Stripe processes personal data necessary to manage the electronic commerce platform and to process payment transactions such as: bank account details, billing/shipping address, name, order description (including date, time, amount, product or service description), device ID, email address, IP address/location, order ID, payment card details, tax ID/status, unique customer identifier, identity information including government issued documents (e.g., national IDs, driver's licences and passports).

Stripe also processes personal data (e.g., name, address, phone number, country) in connection with fraud monitoring, prevention, detection and compliance activities for Stripe and its Business Users. To learn more about the personal data we collect and why visit our Privacy Policy.

If data subjects are provided with access to their personal data, are they able to correct, amend, restrict, or delete that information?

Stripe honours an individual's request to exercise his or her rights under applicable data protection law.

When an End Customer requests you, a Stripe Business User, to delete, share a copy of, or amend their personal information, you can do so immediately through the API or in your Stripe Dashboard. Stripe will in turn help process End Customer data subject requests in accordance with the Business User's written instructions and applicable law, retaining personal data to the extent necessary to comply with our legal and regulatory obligations. We may also retain personal data to allow for fraud monitoring, detection and prevention activities. In cases where we keep personal data, we do so in accordance with any limitation periods and records retention obligations that are imposed by applicable law.

As a Stripe End User, you may have choices regarding our collection, use and disclosure of your personal data as detailed in our Privacy Policy and Stripe Privacy Center. We will comply with your request to the extent required by applicable law.

How is notice provided to data subjects regarding the use of their personal data?

Under the terms of our agreements, Business Users are required to provide all necessary notices and obtain all necessary rights and consents from their End Customers to enable Stripe to lawfully collect, use, retain and disclose the Personal Data as part of the Stripe Services. Business Users, as data controllers, are responsible for the contents of their privacy notice and cookie banner. Learn more.

From where does Stripe collect information used for fraud prevention and security purposes?

To prevent fraud and strengthen our security, we may collect information from Business Users, End Customers, End Users, financial parties, and in some cases third parties. For example, we collect and analyse information that helps us identify bad actors and bots, including both transactional data (such as amount, customer shipping address, date, and so on) and advanced fraud detection signals (device and activity signals). Learn more.

Stripe also receives information from third parties to prevent and respond to security incidents, and for protecting against other fraudulent activity. E.g., we may receive information from third parties about IP addresses that malicious actors have compromised.

Does Stripe sell End Customer personal information under the CCPA?

Stripe does not sell this personal information. As such, we do not have actual knowledge that we sell personal information of minors under 16 years of age. For California residents, the California Consumer Privacy Act (CCPA) defines "selling" personal information to include providing it to a third party in exchange for money or valuable consideration. See Cal. Civ. Code § 1798.140(t)(1).

For Shine the Light law (Cal. Civ Code § 1798.83) purposes, Stripe does not share personal data of California customers to third parties for their direct marketing purposes, as defined by this law. For more information, please see our Privacy Center.

➔ Privacy, data protection and data security trainings and employee compliance

Does Stripe have a training program related to privacy and data protection compliance for Stripe employees?

Yes. All Stripe employees are required to participate in our Annual Security and Privacy training to ensure all Stripe employees are up to speed with our most current security and privacy protocols. Our annual training covers a wide range of topics, including physical security, use of Stripe devices, phishing and security.

Additionally, EMEA based Stripe employees attend Privacy and Security training as a part of onboarding to Stripe. As a result, all Stripe employees are aware of their obligations in regards to processing personal data under applicable data protection law.

Are Stripe employees held accountable to privacy, data protection and data security standards?

Yes. All Stripe employees are subject to our internal guidelines regarding data protection and confidentiality. We have internal tools that hold us accountable to these standards. This is in addition to confidentiality obligations all Stripe employees have to abide by.

Stripe takes its privacy, data protection and data security standards seriously and any failure by a Stripe employee to comply with his/her responsibilities under applicable data protection law will be promptly investigated. Employees who violate applicable law and/or Stripe's internal guidelines will be subject to Stripe's disciplinary procedures.

➔ International Data Transfers

Does Stripe transfer personal data outside of its country of origin?

Stripe is a global service provider and data may be transferred outside of its country of origin as part of our Stripe services, including outside of the EEA, UK and Switzerland.

Data protection laws and regulations vary around the globe. Where Stripe transfers personal data to a country or recipient that is not recognized as having an adequate level of protection for personal data under applicable data protection law, Stripe will ensure such transfers of personal data are made in compliance with applicable law and the contractual terms in place with its Business Users.

Our production data is hosted in data centres in the United States and therefore, the transfers of personal data outside of Europe are necessary to provide the Stripe services, to operate globally and to provide our products and services to any Business User. We adhere to international standards, controls and security measures like compliance with PCI DSS Level 1, multiple ISO standards.

To support Stripe in delivering its global services, we engage service providers, sub-processors and affiliates to assist Stripe with its data processing activities on behalf of our Business Users. As part of Stripe's commitment to privacy and security, our external service providers page includes information about our existing service providers and sub-processors (e.g. their location, privacy statements), and details on how users can subscribe to receive notifications about updates to the page. We also partner with third

parties such as banks, payment method providers (e.g. Visa, Mastercard) and payment processors. Learn more.

How is Stripe dealing with its international data transfers?

Stripe may transfer your Personal Data to countries other than your own country, including to the United States. Stripe relies on a number of data transfer mechanisms to legalise the transfer of Personal Data around the globe.

Stripe's compliance measures to ensure an adequate level of protection of Personal Data transferred outside the UK, EEA and Switzerland. Stripe's measures may include:

- Transferring Personal Data from the originating country to a country or recipient that has been deemed to have an adequate level of data protection by relevant privacy authorities, including the European Commission.
- The EU-U.S. Data Privacy Framework ("EU-U.S. DPF"), which allows personal data to flow freely between the EEA and certified organizations in the U.S. The European Commission has adopted an adequacy decision confirming that personal data can be transferred from the European Economic Area ("EEA") to certified U.S. organizations. The UK Government similarly confirmed that organizations can rely on the UK Extension to the EU-U.S. DPF to transfer data from the UK to certified U.S. organizations. Stripe's parent entity, Stripe, Inc, is certified under the EU-U.S DPF, the Swiss-US Data Privacy Framework ("Swiss-U.S. DPF") and the UK Extension to the EU-U.S. DPF ("UK Extension"). Stripe relies on the DPF to transfer personal data from the EEA and the UK to the US. The Swiss-U.S. DPF will not be relied upon by Stripe until Switzerland recognises its adequacy consistent with Swiss law, but we adhere to its required commitments in anticipation of their doing so. To learn more about the DPF program, please visit https://www.dataprivacyframework.gov/, and to view our certification, please see here.
- The Standard Contract Clauses ("SCCs") approved by the European Commission. SCCs are a transfer mechanism (in the form of a legal contract) used by Stripe to provide a legal mechanism to transfer EU personal data outside of the EEA/UK. These are incorporated into our agreements.
- The UK International Data Transfer Addendum ("UK Addendum") issued by the UK's Information Commissioner's Office to provide a legal mechanism to transfer Personal Data from the UK. The mechanism is required under UK data protection law (known as UK GDPR) and is incorporated into our agreements.
- Other alternative data transfer mechanisms approved by relevant privacy authorities to enable the transfer of Personal Data to a third country.

What are Stripe's supplemental measures to protect personal data from unauthorised access?

Stripe maintains and enforces a security program that addresses the management of security and the security controls employed by Stripe. We also perform risk assessments and implement and maintain controls for risk identification, analysis, monitoring, reporting, and corrective action. Stripe maintains and enforces an asset management program that appropriately classifies and controls hardware and software assets throughout their life

cycle. In addition, Stripe employees, agents, and contractors acknowledge their data security and privacy responsibilities under Stripe's policies.

Stripe applies technical and organisational measures that include the following:

- **Physical access control** to prevent unauthorised persons from gaining access to the data processing systems available at premises and facilities (including databases, application servers, and related hardware), where personal data is processed.
- **Virtual access control** to prevent data processing systems from being used by unauthorised persons.
- **Data access control** to ensure that persons entitled to use a data processing system gain access only to such personal data in accordance with their access rights, and that personal data cannot be read, copied, modified or deleted without authorization.
- **Disclosure control** to ensure that personal data cannot be read, copied, modified or deleted without authorization during electronic transmission, transport or storage on storage media (manual or electronic), and that it can be verified to which companies or other legal entities personal data are disclosed.
- **Entry control** to audit whether data have been entered, changed or removed (deleted), and by whom, from data processing systems.
- **Availability control** to ensure that personal data is protected against accidental destruction or loss (physical/logical).
- **Separation control** to ensure that personal data collected for different purposes can be processed separately.

By default, Stripe encrypts data at rest and data in transit. We further protect your data with tools like audit logs, access management policies and certifications as described on our Payments page in the section "Security and compliance at the core". Security controls implemented at Stripe include TLS 1.2 configuration of endpoints for data in transit, TLS and/or SSL encryption for HTTPS and regular testing of infrastructure components. Two-step authentication is available for an extra layer of security at Dashboard login.

We get requests for access to data from law enforcement, and we review each request with the goal of responding with the minimum amount of required information in response to legitimate, legally mandated requests. To learn more about our commitment to privacy and data security, see our Privacy Policy, Privacy Center, and Security Centre.

➔ Data classification

Does Stripe have a data classification system that identifies different classes of information based on sensitivity?

Yes, Stripe has a data classification policy. Stripe classifies data based on access rights and access rights limitations. To point out specifically, cardholder data is stored in an entirely separated production environment than the remainder of our data. This is for PCI compliance reasons. This environment has a small number of Stripe employees with appropriate production access, and shares no common credentials with our non-cardholder environment. Stripe allows only authorised individuals to access any environments and secure data centres that process personal data.

➔ Data Retention

Does Stripe have rules and procedures around data retention?

Yes, Stripe retains personal data in compliance with applicable data protection laws, and additional sector-specific rules, that apply to Stripe.

Stripe is subject to anti-money laundering and financial regulatory obligations that require Stripe to retain transactional records for specified periods. When personal data is no longer needed to perform the requested services or satisfy regulatory requirements, it is securely and automatically removed from our systems.

When determining the relevant retention periods, we will consider various criteria such as your location, the nature of our relationship with you, the types of products or services being offered or provided to you, the nature and sensitivity of your personal data, the mandatory retention periods provided by law or statute of limitations and any overriding legitimate grounds for continuing to retain the personal data (such as defending our rights in court, enforcing our agreements, detecting fraud or complying with valid legal process requests from courts or competent authorities).

For most jurisdictions, Stripe will generally keep personal data related to Business Users for a period of five or more years from the end of the business relationship with you, or the date of the last transaction, whichever is later. For more information about our data retention practices, please visit our Privacy Policy.

➔ Audit Rights

Does Stripe allow Business Users to audit Stripe's compliance with data protection law?

Stripe will facilitate client requests for audits and inspections in accordance with the terms of the Data Processing Agreement between Stripe and the relevant Business User.

➔ Risk Assessment Processes

Does Stripe conduct privacy risk assessments?

Yes. Our Engineering, Product, Safety, Security and Legal teams collaborate very closely and have developed internal processes and procedures to perform such privacy risk assessments where appropriate.

➔ Data Processors/ Service Providers

Who are Stripe's sub-processors?

Please see our service providers page where we have a list of our most common sub-processors, service providers and affiliates.

How does Stripe replace or designate a new sub-processor?

We will periodically update our sub-processor list to reflect any changes or additions to Stripe's sub-processors. If you are a Business User, you may subscribe to receive email notifications of updates to our service providers page here.

Does Stripe have appropriate contractual controls to demonstrate that personal data shared with third parties is appropriately protected by the third party?

Yes. Stripe has an internal vendor management program in place that allows us to understand who our vendors are, and whether their services provided to Stripe trigger GDPR obligations. If that is the case, we have established a comprehensive set of Art. 28 GDPR-compliant terms that our sub-processors are required to sign before they can process personal data.

Are third-party service providers regularly monitored for privacy compliance?

Yes. In accordance with applicable law, we generally reserve ourselves the right to verify the compliance of our service providers on a regular basis. Stripe identifies, evaluates, and engages third party service providers through our program. We enter into a contract with each provider prior to sharing data as applicable, and each contract contains terms that provide for monitoring and audit. In addition, all potential providers are vetted and approved through Stripe's security review process before we begin using their services.

➔ Data Processing Agreement

I have a Data Processing Agreement – can Stripe agree to that?

We understand that our Business Users have undergone due diligence and may have prepared their own Data Processing Agreements (DPA) for their third party service providers to sign.

However, as a platform provider, we need to ensure consistency across our platform, and that includes consistency with respect to the commitments that we give about how we operate our platform. The fundamental purpose of a DPA is to describe how information is shared and processed, and the Stripe DPA describes how information is shared and processed on the Stripe platform.

Given the nature of the services we provide and our role as a data controller and as a data processor for different data processing activities relating to our platform, we require our Business Users (incl. Platforms) to use our bespoke DPA, as this document better describes the functionality of our platform and our relationship with our Business Users (and Platforms). We make our DPA available to Business Users. Please contact us or your account manager for more detail.

➔ Compliance and Regulatory

Are there requirements to comply with any legal, regulatory or industry requirements, such as Card Network Rules or PCI-DSS?

Yes, as a payment service provider, Stripe is required to comply with applicable card network rules (for example, those rules published by Visa, Mastercard and American Express) as well as rules applicable to other payment methods (such ACH and BACS). In particular, the card network rules prescribe that Stripe must maintain all materials or records in any form that contains cardholder or transaction information in a safe and secure manner with access limited to authorised personnel, as specified in the Payment Card Industry Data Security Standard (PCI-DSS). The card network rules also require that Stripe ensure that all

of its agents and merchants with access to cardholder or transaction information comply with PCI-DSS. For more information, see Security at Stripe.

➔ Security and incident management

Is there more information on Stripe's approach to security?

Stripe has appropriate security in place to prevent the personal data it holds being accidentally or deliberately compromised. Such security measures relate to both the protection of our networks and information systems from attack, and physical and organisational security measures. For more information, see Security at Stripe.

Is there an Incident Response Plan?

Yes. The Stripe Incident Response plan is kept current and outlines our processes and procedures in case of an incident. Stripe employees receive training on how to handle an incident in accordance with the Incident Response Plan.

Is there a Business Continuity / Disaster Recovery program?

Yes. Stripe Technology Europe, Limited is regulated as an electronic money institution by the Central Bank of Ireland and also passports its regulated services across the EEA. In the UK, Stripe Payments UK Ltd is an electronic money institution authorised and supervised by the Financial Conduct Authority in respect of its regulated services. Both entities maintain state-of-the-art business continuity and disaster recovery programs which are reviewed and updated regularly.

Is there an Information Security Policy?

Yes, Stripe maintains an Information Security Policy and a Cybersecurity Policy. The Information Security Policy outlines Stripe's steps taken to protect information, triaged by types of sensitivity. Our Cybersecurity Policy governs the approach Stripe takes to data governance and classification, asset inventories, access controls and identity management, business continuity and disaster recovery asset management, and other elements related to these.

Is there insurance coverage for business interruptions related to cybersecurity incidents?

Yes, Stripe maintains insurance coverage in the event of business interruptions related to cybersecurity incidents. Any insurance cover is subject to the terms of the relevant policy.

What will Stripe do in the event of a security incident?

In relation to the personal data we process on a Business User's behalf as a data processor, we will notify the Business User (as they are the data controller) of a security incident without undue delay or as otherwise specified in our Data Processing Agreement with you.

Are security roles and responsibilities of constituents defined and documented in accordance with Stripe's Information Security Policy?

Yes, we have clearly defined roles and responsibilities and the members of the security team engage in regular table top exercises to practice incident response processes and procedures.

➔ Cookies

Does Stripe use cookies?

Yes, we use cookies to ensure that our Services function properly, to prevent and detect fraud and violations of our terms of service, to understand how visitors use and engage with our website and analyse and improve the Services. Cookies play an important role in helping Stripe provide personal, effective and safe Services.

Depending on an individual's relationship with Stripe and the domains they're visiting, different cookies apply. To comply with our own transparency requirements, we explain how Stripe uses cookies in our Cookie Policy and our Cookies Settings Dashboard sets out our up-to-date list of cookies. Some cookies are set on the public Stripe domain, some on the Dashboard when an individual is logged in as a Stripe Business User, and some on the Business User's website pages (including the payment page) available to customers who make payments. We advise Stripe Business Users to always check our Cookie Settings Dashboard for the most up-to-date information.

Which cookies are installed?

The cookies that are set on a Stripe Business User's site depend on the type of product or service they choose. For example, you can see Stripe Docs for guidance on how to integrate Checkout here: https://stripe.com/docs/payments/checkout and read through the Radar integration checklist.

If a User includes stripe.js on their site pages (by loading stripe.js), then fraud signals are set on the User's domain and process data of visitors to that domain. See below more information about these cookies.

How information is collected: Stripe.js includes 3 cookies that are set for fraud prevention purposes: _stripe_mid, _stripe_sid, and m.stripe.com (called _guid/ m cookie). As described in our Advanced Fraud Detection documentation, we collect fraud signals through Stripe.js and our mobile SDKs to detect and prevent fraud. Stripe.js is a JavaScript library that businesses use to integrate Stripe and accept online payments. Once Stripe.js or our mobile SDKs are added to a site or mobile app, fraud signals are used to differentiate legitimate behaviour from fraudulent behaviour. All three cookies are first party cookies as can be seen in our Cookies Settings page: https://stripe.com/cookie-settings

Purpose of processing: The purpose of this data processing is to prevent fraud by reducing the number of fraudulent transactions and enabling legitimate transactions. Thus, consequently protecting businesses by securing transactions and enabling a safer e-commerce environment. This advanced fraud detection signal data is never used for advertising and won't be rented, sold, or given to advertisers, as outlined in our privacy policy.

When are the cookies set: This depends on how you choose to integrate Stripe.js in your website. The __stripe_sid, __stripe_mid, and m cookies are set shortly after Stripe.js is loaded on the page.

Your choices: As a site owner, you have the ability to disable advanced fraud detection signals if you choose so. If applicable, please see this Radar integration checklist to understand how Stripe Radar is integrated, including some draft disclosure language to End Customer.

➔ Stripe entities

Which Stripe entities are involved?

For most of our services, it is either Stripe, Inc., the US parent company operating under US law, or Stripe Payments Europe, Limited (SPEL), an Irish company operating under Irish law, the data controller responsible for personal data collected and processed in relation to Stripe services.

The Stripe entity responsible for your data will depend on your location, the product or service you use with us and whether Stripe is acting as a controller and/or data processor.

If you are located outside of the Americas (e.g., the EEA, Switzerland or the United Kingdom, countries located in Asia Pacific), SPEL is the primary entity responsible for the processing of your personal data. Some of the payment processing services offered by SPEL are services that may be only provided for by an authorised payment services provider or electronic money institution. In this case, SPEL and the Stripe local regulated entity (defined as those who are licensed, authorised or registered by a Local Regulatory Authority) will act as joint controllers of your personal data. Learn more.

Stripe affiliates also provide local support services in certain countries where Stripe operates. These entities act as data processors on behalf of Stripe, Inc. or SPEL, depending on the jurisdiction. You will find the most up-to-date list of our Stripe affiliates on this page.