Shopify GDPR Whitepaper

April 20, 2018

shopify

Disclaimer

Please note that this document is provided for informational purposes only. Its contents may be subject to change over time. The information in this whitepaper does not modify existing contractual arrangements and may not be construed as legal advice.

Table of contents

Introduction

Shopify is working to make sure that it will comply with the European Union's General Data Protection Regulation (GDPR) when it takes effect on May 25, 2018, and to make sure that its merchants will also be in a position to comply in relation to their use of Shopify. This whitepaper presents Shopify's approach to GDPR preparation and compliance.

Terms

BCRs: Binding Corporate Rules.
Buyer: Person visiting a store hosted by Shopify.
Controller: Party that determines how and for what purposes personal data is processed.
Data subject: Person about whom personal data relates.
DPIA: Data Protection Impact Assessment.
EEA: European Economic Area. EEA countries currently include Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, and the United Kingdom.
GDPR: General Data Protection Regulation.
Merchant: Party using Shopify to host their store.
NDA: Non-disclosure Agreement
Partner: Party that creates Shopify stores on behalf of merchants.
Personal data: Any information relating to an identified or identifiable person.
PIPEDA: Personal Information Protection and Electronic Documents Act.
Processor: Party that processes personal data on behalf of the controller.

Global GDPR application

Who does the GDPR apply to?

Shopify

The GDPR applies to any company that handles the personal data of residents in the European Economic Area (EEA). Because Shopify works with merchants who serve buyers in the EEA, and serves buyers in the EEA directly, the GDPR applies to these elements of its business.

However, because Shopify believes strongly in data protection and privacy, it will give all of its merchants and partners the ability to offer their buyers the rights afforded by the GDPR to control their personal data, wherever they live. Additionally, Shopify will provide tools and processes for its merchants to fulfill GDPR-related requests from their buyers regardless of the buyer's location.

Merchants and partners

Separate from the way in which the GDPR applies to Shopify, the regulation also applies to Shopify's merchants and partners who operate in the EEA or offer goods or services to residents of the EEA.

While Shopify is working to make sure that its own operations will comply with the GDPR, and to provide its merchants and partners with the tools to help its merchants comply with the GDPR, each merchant is ultimately responsible for ensuring that their business complies with the laws of the jurisdictions in which they operate or have buyers.

Using Shopify does not guarantee that a merchant or partner complies with the GDPR.

Buyers

The GDPR also gives certain rights to identified or identifiable persons (referred to as *data subjects*), including buyers visiting stores belonging to Shopify merchants. These include the right to request:

- Deletion (*erasure*) of their personal data
- Correction (*rectification*) of their data
- Access to their data
- An export of their data in a common (*portable*) format

This topic is discussed more fully in the **Data subject rights** section.

What data does the GDPR apply to?

The GDPR generally applies to the collection and processing of personal data. Under the GDPR, *personal data* means any information relating to a data subject. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as:

- Name
- Identification number
- Location data
- Online identifier (such as IP address or cookie ID)[1]

Controller vs. processor status

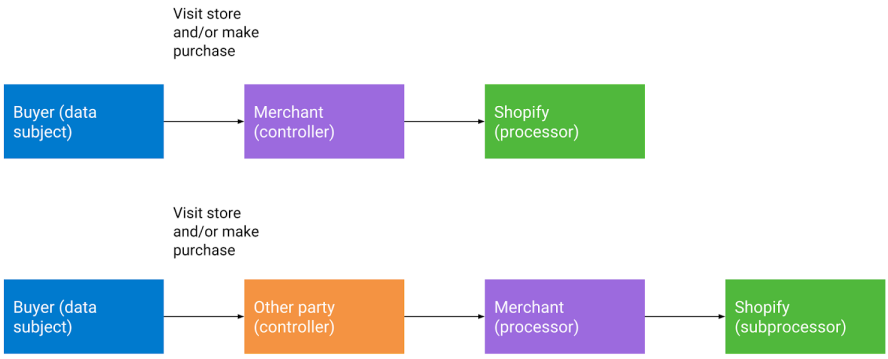
The GDPR separates data protection responsibilities into two categories: controllers and processors.

Controller: The party that determines for what purposes and how personal data is processed.[2]

[1] General Data Protection Regulation, Article 4(1).
[2] General Data Protection Regulation, Article 4(7).

Processor: The party that processes personal data on behalf of the controller.[3]

Under the GDPR, in most cases the merchant collects information from their buyers as a controller. Generally, Shopify acts as a processor for the merchant with respect to such buyer personal data (or, if the merchant acts as a processor, Shopify acts as a subprocessor):

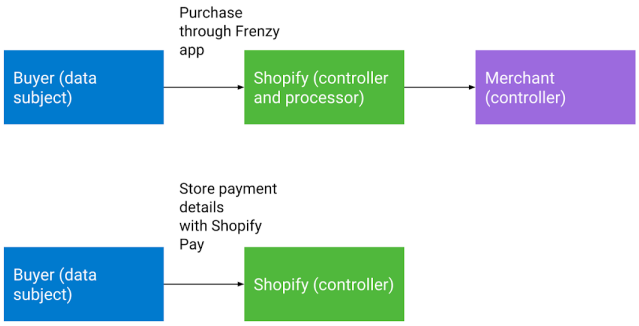


The one exception is for buyers with whom Shopify has a direct existing relationship. For example:

- Buyers who use Shopify's Frenzy flash-sale app to access a merchant's store
- Buyers who use Shopify Pay, which allows the buyer to store their payment information with Shopify for use across different Shopify stores
- Buyers who use Shopify's Arrive app to track the status of orders made from a merchant's store

Although in such cases the merchant may also separately be a controller of the buyer's personal data, Shopify processes the personal data of these buyers as a controller, as indicated in the following diagram:

[3] General Data Protection Regulation, Article 4(8).



Processor obligations

To comply with the GDPR, generally the processor may only process personal data when authorised to do so by the controller.

Where Shopify is a processor for a merchant, it processes personal data on documented instructions from merchants. For example, when a merchant clicks **Fulfill items**, they give Shopify the instruction to process the data necessary to perform that action.[4]

Similarly, when a merchant selects a particular payment processor, or installs an application through the Shopify app store, they give Shopify the instruction to transmit data to the relevant party.

The GDPR also places several other responsibilities on the processor, discussed below:

[4] See section 2.2.1 of Shopify's Data Processing Addendum: https://www.shopify.com/legal/dpa.

Subprocessing

Processors must notify and obtain consent from their controller when transmitting personal data to a subprocessor. Shopify uses a number of subprocessors to provide the service, including to:

- Store platform data
- Operate the forums and other portions of Shopify's website
- Respond to and manage support inquiries

When a merchant signs up for the Shopify service, they consent to allow Shopify to use subprocessors. A list of subprocessors is available upon request.

Data protection impact assessments

Shopify is formalising the process for conducting data protection impact assessments (DPIAs) any time a change in processing procedure occurs that is likely to result in a high risk to individuals' privacy rights. Shopify will help answer reasonable questions a merchant has about Shopify's processing activities.

Personal data breach reporting

Processors must notify the controller after becoming aware of a personal data breach resulting from a breach of the processor's security.

Shopify is committed to ensuring that its incident response program meets the requirements of the GDPR. The specifics of breach notification are handled through a merchant's contract with Shopify.

Appointment of a Data Protection Officer

Processors must appoint a Data Protection Officer if they conduct certain types of personal data processing.

Shopify's Data Protection Officer can be reached at privacy@shopify.com. Merchants should consider whether they also need to appoint a Data Protection Officer.[5]

Controller obligations

Under the GDPR, the controller has the following responsibilities:

Facilitating requests

Controllers are obligated to help data subjects exercise their rights.[6]

Shopify's merchants can do this by forwarding buyer requests to Shopify, as detailed in the **Data subject rights** section of this document.

Posting a privacy notice

When personal data is collected from a data subject, controllers must provide certain minimum information about the intended processing of the personal data, as well as information about how to contact and identify the controller.[7]

Merchants are responsible for providing this information to their buyers. Shopify provides this information in the Shopify Privacy Policy where it is

[5] General Data Protection Regulation, Article 37.
[6] General Data Protection Regulation, Article 12(2).
[7] General Data Protection Regulation, Article 13.

a controller, and encourages merchants to provide this information in their own privacy policies.[8]

Complying with marketing and cookie regulations

Controllers are responsible for making sure that they comply with marketing and cookie regulations in the jurisdictions in which they operate.

Merchants with EU buyers should make sure that they obtain appropriate consent for the use of cookies—the ePrivacy Directive generally requires some form of consent in order to use tracking technologies.[9]

All merchants should similarly make sure that their email marketing practices comply with applicable e-marketing or anti-spam requirements.

Obtaining consent to process children's data

When offering goods or services online directly to children under 16 years of age, the controller is responsible for obtaining verifiable consent from the child's parents for processing their data.[10]

Merchants are responsible for assessing whether they need to obtain a higher level of consent for certain buyers.

Legal basis for processing

Personal data cannot be processed except under a recognized legal basis (unless an exemption applies). The GDPR sets out a list of possible legal

[8] Shopify's Privacy Policy: https://www.shopify.com/legal/privacy.
[9] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). Will be replaced by the ePrivacy Regulation.
[10] General Data Protection Regulation, Article 8. Individual member states may lower the age of consent.

bases under which personal data may be processed. These reasons include:

- Consent
- Contractual obligations
- Legal obligations
- The public's interests
- Legitimate interests of the controller or third party, balanced against the rights of the data subject[11]

Consent of the data subject means the data subject has agreed to the processing of their personal data with a clear affirmative action.[12]
This agreement must be:

- Freely given
- Specific
- Informed
- Unambiguous

Merchants, as controllers of their buyers' personal data, are responsible for ensuring they have a proper legal basis for doing so, including keeping evidence of consent when processing is based on consent.[13]

As its merchants' processor, Shopify is not responsible for the merchants' legal bases but only processes buyers' personal data on behalf of and on the instructions of the merchant. In certain cases, however, the law may additionally require consent for certain types of processing (for example, when placing or retrieving cookies on a device). In such cases, the merchant is also responsible for obtaining appropriate consent.

[11] General Data Protection Regulation, Article 6.
[12] General Data Protection Regulation, Article 4(11).
[13] General Data Protection Regulation, Article 7(1).

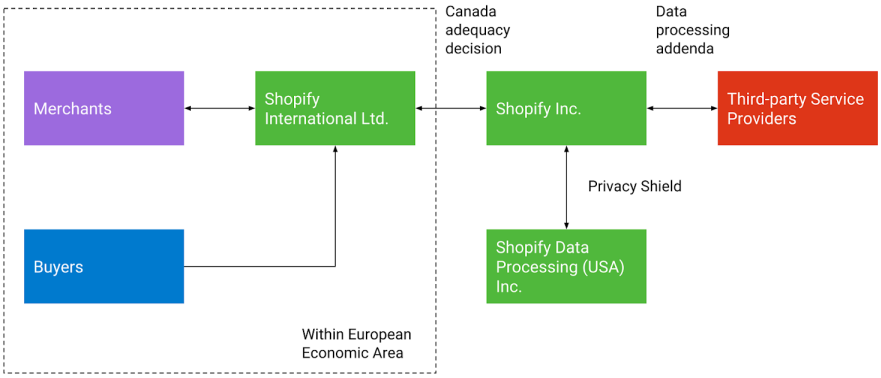
Upon request, Shopify will provide merchants with any reasonable information they require to obtain consent (for example, information about the categories of cookies placed when a buyer visits a storefront).

Data transfers

Personal data of residents of the EEA can only be transferred to recipients outside the EEA if the recipient has adequate protections in place. These protections may include:

- Adherence to domestic laws that have been deemed adequate by the European Commission
- Negotiated agreements (such as the EU-U.S. Privacy Shield)
- Contractual protections
- Approved sets of internal policies (Binding Corporate Rules)
- Approved codes of conduct or certifications

Shopify has protections for personal data in every step of its data flow, as described below. The following diagram illustrates Shopify's data transfer structure:



Within EEA

EEA personal data is received and initially processed by Shopify's Irish entity, Shopify International Ltd.

EEA to Canada

Data is exported from the EEA to Shopify's Canadian parent entity, Shopify Inc. This export takes place within Shopify's corporate structure.

Data within Shopify Inc. is protected under PIPEDA, Canada's private sector privacy legislation, which is considered adequate under the GDPR.[14]

United States

Shopify Inc. uses a combination of data centers and cloud service providers to store this personal data in the United States and Canada.

When personal data is transferred to the United States, it is either done so through the EU-U.S. and Swiss-U.S. Privacy Shield, for Shopify's own storage, or through contractual data protection addenda (DPAs) with third-party service providers. The EU-U.S. and Swiss-U.S. Privacy Shields are also considered adequate under the GDPR. Shopify's Privacy Shield certification statement can be found on PrivacyShield.gov.[15]

---

[14] Pursuant to the European Commission's adequacy decision 2002/2/EC. Commission Decision of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act (notified under document number C(2001) 4539), online at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32002D0002&qid=1415699250815.

[15] See: https://www.privacyshield.gov/participant?id=a2zt0000000TNSNAA4.

Additionally, Shopify is in the process of applying for approval of Binding Corporate Rules (BCRs) by the Irish Data Protection Commissioner. After they are approved, Shopify will rely on these BCRs to protect the personal data that is transferred between Shopify's corporate entities worldwide.

Disclosures to third parties

Shopify will never independently sell personal data for commercial purposes. However, Shopify does disclose personal data to third parties or allow third parties to access personal data to help provide services—for example, to:

- Store platform data
- Operate the forums and other portions of Shopify's website
- Respond to and manage support inquiries

Additionally, Shopify may provide personal data, where permitted, to prevent, investigate, or respond to:

- Potential fraud
- Illegal conduct
- Physical threats
- Violations of any agreements with Shopify

Shopify also provides information to third parties when legally required to do so. Where Shopify believes it is legally required to provide information, and not legally prohibited from disclosing the existence of the legal order, it will notify the data subject and give the data subject a chance to seek a protective order.

More information on when Shopify discloses personal data will soon be provided on Shopify's website under the heading **Guidelines for Legal Requests for Merchant or Buyer Data**.

Shopify ecosystem

If a merchant agrees to use a third-party service provider such as a payment processor, a sales channel, or an app that is not controlled by Shopify, the respective service provider's use of personal data is controlled by the merchant's agreement with the provider. Shopify is not responsible for the data practices of these third-party service providers, and merchants should carefully evaluate these service providers as they would any third party.

Shopify recognises that it might be difficult for some merchants to obtain enough information from these service providers to conduct a careful evaluation. Shopify is working with these providers to make sure that they make information available to merchants about their data practices.

App Store disclosures

Similarly, Shopify is requiring all apps on the Shopify App Store to post disclosures about how the app handles personal data, but Shopify is not responsible for any app's data collection or use, or for how the merchant uses the app. The merchant is responsible for reviewing these disclosures and to ensure that their use of the app complies with the laws of the jurisdictions in which the merchant operates or where it has buyers.

Data subject rights

The GDPR provides data subjects (in this case, buyers) with certain rights over their personal data. Generally, data subject requests must be addressed within one month, unless they are exceptionally complex or numerous.[16] The following rights are granted to data subjects:

[16] General Data Protection Regulation, Article 12(3).

Erasure

Data subjects have the right to request that their personal data be erased in certain circumstances.

If a merchant receives a request from a buyer to delete their personal data, before forwarding the request to Shopify, the merchant should:

- Verify that the requester is the same as the data subject (that is, the requester is not asking to erase someone else's personal data)
- Confirm there is no legal reason to preserve this data

If both conditions are satisfied, the merchant should forward the request to Shopify, either through Shopify's support system, or by emailing privacy@shopify.com.

After a request is received, Shopify will ensure that the relevant personal data is erased. If erasing it is impossible, Shopify will let the merchant know to what degree it is impossible, and why.

In addition to contacting Shopify, the merchant should also work with any relevant third parties to make sure that they delete or anonymise the personal data.

Timing

Personal data cannot be erased from Shopify while it is:

- Associated with a pending order
- Associated with an order made fewer than 180 days before the request (the usual window in which a buyer can make a chargeback).

If the buyer's personal data cannot be erased for this reason, the merchant should re-submit the deletion request after the appropriate time has passed.

Scope

When processing a request for erasure, Shopify will anonymise the personal data of the buyer, but keep non-personal data such as revenue information and order details. Order details that are retained include the gateway used to process payment, time of sale, amount paid, currency, subtotal, shipping cost, taxes added, shipping method, item quantity, item name, SKU, and payment method.

If no data erasure requests are received, Shopify will keep data for the lifetime of a store, and purge personal data within 90 days after a store is closed.

Access

Controllers must, upon request, explain to data subjects how their personal data is processed and provide access to this personal data.

If merchants cannot export data sufficient to fulfill the request from their admin, they can forward the request to Shopify. Similar to a request for erasure, if a buyer requests access to their personal data, the merchant should first validate the identity of the requester.

The merchant can then reach out to Shopify, either through Shopify's support system, or by emailing privacy@shopify.com.

When Shopify receives the request, it will:

- Confirm whether personal data about a buyer is being processed by Shopify

- Confirm what categories of data are being processed by Shopify
- Provide the buyer with the relevant information from Shopify systems

Data portability

Controllers who process data using automation must, in limited circumstances, provide data subjects with their personal data upon request. This data must be provided in a commonly used and machine-readable format.

Merchants may export some data directly from their store's admin page. Many data types can be exported to common formats such as Excel or CSV with one click:

- Transaction histories
- Payouts
- Product lists
- Customer lists

In addition, if a merchant contacts Shopify to request copies of processed data, Shopify will make the data available in a common format.

Rectification

Data subjects have the right to correct incomplete or inaccurate personal data held or processed by a controller.[17]

Shopify's platform allows a merchant to change customer records directly from their store admin.[18]

[17] General Data Protection Regulation, Article 16.
[18] However, current orders cannot be modified.

Automated decision-making

Data subjects have the right to object to processing based solely on automated decision-making (which includes profiling), when that decision making has a legal effect on the data subject or otherwise significantly affects them.[19] An example of a legal effect is a decision that impacts an individual's legal or civil rights, or their rights under a contract. Examples of significant effects include decisions that have a financial impact on individuals, or impact their employment.

Shopify does not currently engage in fully automated decision-making that has a legal or otherwise significant effect using buyer data.

Services that include elements of automated decision-making are highlighted in the table below:

Service	**Implementation details**
Temporary blacklist of IP addresses associated with repeated failed transactions	Persists for a small number of hours.
Temporary blacklist of credit cards associated with blacklisted IP addresses	Persists for a small number of days.

Data protection and security

Under the GDPR, controllers and processors are required to implement appropriate technical and organisational measures.[20]

[19] General Data Protection Regulation, Article 21.
[20] General Data Protection Regulation, Article 25, 32.

Shopify has implemented many of the controls and processes identified in the GDPR, including:

- Anonymising and encrypting personal data
- Ensuring confidentiality, integrity, availability, and resilience of processing systems
- Restricting who may access personal data
- Ensuring availability and access to personal data in the event of a physical or technical incident
- Performing regular testing, assessments, and evaluation of technical and organisational security measures

Organisational measures

Shopify has a robust, cross-functional data protection program that is integrated with its information security program and includes several teams across the organisation. In particular, the data protection program includes a designated Data Protection Officer, who reports to senior management, as well as individuals from:

- Internal Security
- Legal
- Legal Operations
- Production Security
- Processing Integrity

Technological measures

Monitoring and logging

Controllers—and where applicable, their representative—must maintain records of the personal data processing activities for which they are responsible.

Shopify maintains system and application logs relating to events and access to certain systems used for the processing of personal data. These logs are stored on log servers for approximately a month, and then moved to offsite backup locations, where they remain available for at least 12 months.

Security controls

Shopify encrypts data sent to and from merchants and buyers using the HTTPS protocol.

Shopify also encrypts any sensitive stored information, and salts and hashes merchant and buyer passwords using bcrypt.

Merchants can also set up additional security features. An account holder can take the following actions from their Shopify admin:

- Enable multi-factor authentication for staff
- Define, to a certain extent, what personal data is collected from buyers
- View certain activity logs, including recent login activity by staff
- Set role-based permissions for staff accounts

Security standards and certifications

Shopify and all online stores powered by Shopify are Level 1 PCI-DSS compliant.[21]

Shopify uses third-party data centers with industry-standard certifications. Examples include:

[21] See: https://www.shopify.ca/pci-compliant.

- Tier III
- ISO 27001
- PCI-DSS

SOC reports for all facilities, which include physical protections, can be provided to merchants on request under an appropriate NDA.

Contractual agreements and data processing addenda

Shopify's Terms of Service, Data Processing Addendum, Privacy Policy, and Acceptable Use Policy can be found online at https://www.shopify.com/legal.

Shopify plans

For merchants whose relationship with Shopify is governed by Shopify's online Terms of Service, Shopify has automatically incorporated a Data Processing Addendum, which will apply to its processing of personal data. Just as Shopify is not able to negotiate its Terms of Service, it is not able to negotiate this Data Processing Addendum.

Shopify Plus plans

For Shopify Plus merchants, their negotiated contract will govern their relationship with Shopify. Merchants can sign a Data Processing Addendum to address their needs. Shopify Plus merchants that have not already signed a Data Processing Addendum with Shopify and would like to do so should reach out to their Merchant Success Managers. Shopify Plus merchants that do not sign a Data Processing Addendum will be

governed by Shopify's online Data Processing Addendum (which is incorporated by reference into our online Terms of Service).

Accountability and transparency

Shopify is compiling data for a transparency report, to be released at the end of 2018.

FAQ

What do I do if I have more questions about the GDPR or my local privacy laws?

Contact a local lawyer who specializes in privacy or data protection law.

Who can I contact for more information on Shopify's practices?

Contact privacy@shopify.com.

If I use Shopify to host my store, does my business comply with GDPR?

Not automatically. While Shopify's operations will comply with the GDPR, and Shopify will provide tools to help its merchants comply, it is the responsibility of each merchant to ensure that its business is compliant with the laws of the jurisdiction in which it operates.

Using Shopify's platform alone does not guarantee that a company complies with the GDPR.

Will Shopify sign Standard Contractual Clauses?

No. As described in the **Data transfers** section of this document, Shopify has structured its data flows so that merchants transfer data to Shopify's Irish affiliate within Europe. For that reason, Standard Contractual Clauses are not appropriate, as they are approved for transfers between a European party and a non-European party.

In addition, regarding transfers directly to Shopify Inc., Shopify would rely in such cases on the European Commission's adequacy decision regarding Canada's privacy law, which extends to Shopify Inc. as a Canadian corporation.