

# Shopify GDPR Whitepaper

June 2, 2020



# Table of contents

<b>Disclaimer</b>	<b>2</b>
<b>Introduction</b>	<b>2</b>
Terms	2
<b>Global GDPR application</b>	<b>2</b>
Who does the GDPR apply to?	2
What data does the GDPR apply to?	3
<b>Controller vs. processor status</b>	<b>3</b>
Processor obligations	5
Subprocessing	5
Data protection impact assessments	5
Personal data breach reporting	5
Appointment of a Data Protection Officer	5
Controller obligations	6
Facilitating requests	6
Posting a privacy notice	6
Complying with marketing and cookie regulations	7
Obtaining consent to process children's data	7
<b>Legal basis for processing</b>	<b>8</b>
<b>Data transfers</b>	<b>8</b>
Within EEA	9
EEA to Canada	9
United States	9
Disclosures to third parties	10
Shopify ecosystem	10
App Store disclosures	11
<b>Data subject rights</b>	<b>11</b>
Erasure	11
Timing	11
Scope	12
Access	12
Data portability	12
Rectification	13
Automated decision-making	13
<b>Data protection and security</b>	<b>13</b>
Organisational measures	14
Technological measures	14
Monitoring and logging	14
Security controls	14
Security standards and certifications	14
<b>Contractual agreements and data processing addenda</b>	<b>15</b>
Shopify plans	15
Shopify Plus plans	15
<b>Accountability and transparency</b>	<b>15</b>

# 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.

## Introduction

Shopify believes strongly in protecting your and your customers' personal data, and understands that doing so is critical to help you preserve the trust and confidence of your customers. This whitepaper presents Shopify's approach to GDPR preparation and compliance.

## Terms

**BCRs:** Binding Corporate Rules.

**Controller:** Party that determines how and for what purposes personal data is processed.

**Customer:** Person visiting a store hosted by Shopify.

**Data subject:** Person about whom personal data relates.

**DPIA:** Data Protection Impact Assessment.

**EEA:** European Economic Area. EEA and European Union countries currently include Austria, Belgium, Bulgaria, Croatia, 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 customers in the EEA, and serves customers in the EEA directly, the GDPR applies to these elements of its business.

However, because Shopify believes strongly in data protection and privacy, it gives all of its merchants and partners the ability to offer their customers the rights afforded by the GDPR to control their personal data, wherever they live. Additionally, Shopify provides tools and processes for its merchants to fulfill GDPR-related requests from their customers regardless of the customer'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.

Each merchant is ultimately responsible for ensuring that their business complies with the laws of the jurisdictions in which they operate or have customers.

Using Shopify alone does not guarantee that a merchant or partner complies with the GDPR - merchant and customers must analyse their own business practices to ensure their compliance.

### Customers

The GDPR also gives certain rights to identified or identifiable persons (referred to as *data subjects*), including customers 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)<sup>1</sup>

## 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.<sup>2</sup>

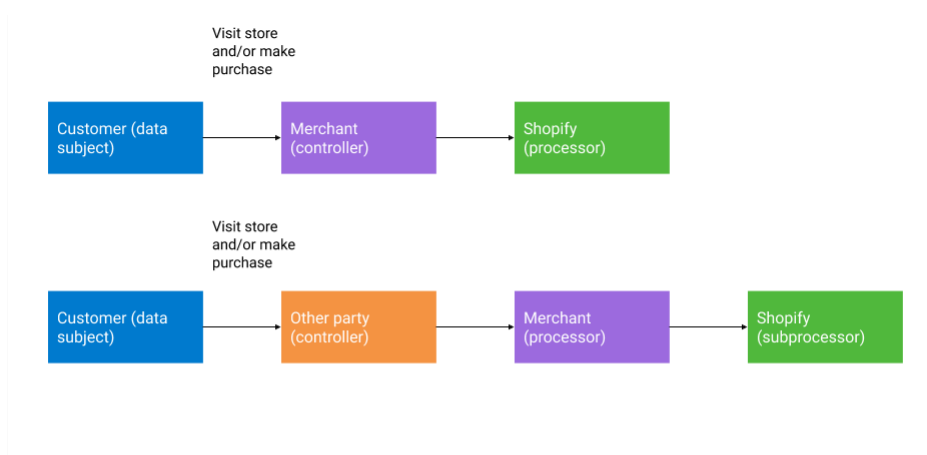
**Processor:** The party that processes personal data on behalf of the controller.<sup>3</sup>

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

<sup>1</sup> General Data Protection Regulation, Article 4(1).

<sup>2</sup> General Data Protection Regulation, Article 4(7).

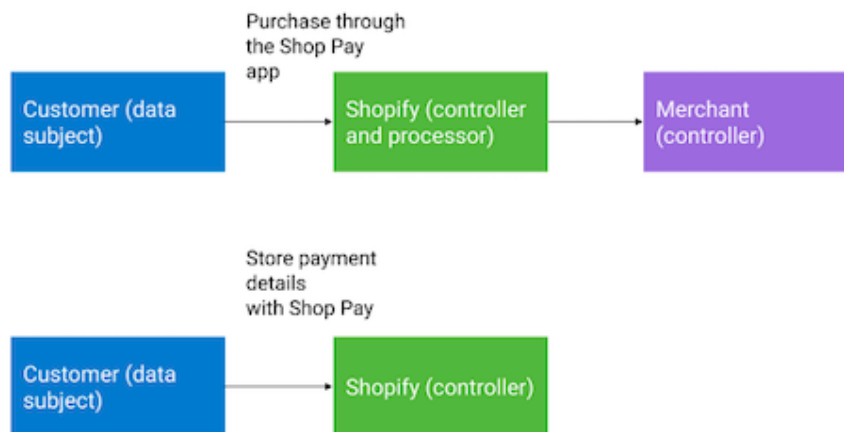
<sup>3</sup> General Data Protection Regulation, Article 4(8).



The one exception is for customers with whom Shopify has a direct existing relationship.

For example, customers who use Shopify's Shop Pay service, which allows the customer to store their payment information with Shopify for use across different Shopify stores, track packages, and find new Shopify stores near them.

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



# 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.<sup>4</sup>

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:

## 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 published in Shopify's Help Center.<sup>5</sup>

## 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](mailto:privacy@shopify.com). Merchants should consider whether they also need to appoint a Data Protection Officer.<sup>6</sup>

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

<sup>5</sup>See: <https://help.shopify.com/manual/your-account/GDPR/subprocessors>

<sup>6</sup>General Data Protection Regulation, Article 37.

# Controller obligations

Under the GDPR, the controller has the following responsibilities:

## Facilitating requests

Controllers are obligated to help data subjects exercise their rights.<sup>7</sup>

Shopify's merchants can do this easily from their admin 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.<sup>8</sup>

Merchants are responsible for providing this information to their customers. Shopify provides this information in the Shopify Privacy Policy where it is a controller, and encourages merchants to provide this information in their own privacy policies.<sup>9</sup>

### Customers

Shopify collects the following elements of personal data from customers on behalf of merchants:

- Name
- Shipping and billing addresses
- IP address
- Customer email or phone number (if required by merchant)
- Company name (if required by merchant)
- Information from cookies, stored temporarily as per Shopify's Cookie Policy (for example, which landing page the customer arrived from, how many times the customer has visited the site, device and browser used, and products stored in the cart)<sup>10</sup>
- Information about the orders customers initiate so that Shopify may fulfill those orders.

If a customer contacts Shopify for customer support, Shopify also collects the following information:

### Telephone support

Shopify collects:

- Phone number
- Call audio
- Other personal information provided during the call

In accordance with Shopify's Terms of Service, Shopify may request additional documentation during the call to verify identity.<sup>11</sup>

<sup>7</sup>General Data Protection Regulation, Article 12(2).

<sup>8</sup>General Data Protection Regulation, Article 13.

<sup>9</sup>See: <https://www.shopify.com/legal/privacy>.

<sup>10</sup>See: <https://www.shopify.ca/legal/cookies>.

<sup>11</sup>See: <https://www.shopify.com/legal/terms>.

### Chat support

Shopify collects:

- Name
- Email address
- Information about the device and browser used
- Network connection
- IP address
- Chat transcript
- Other personal information provided during the chat

In accordance with our Terms of Service, Shopify may request additional documentation during the chat to verify identity.<sup>12</sup>

### Forums

Shopify collects:

- Name
- Email address
- Website URL
- Other personal information the user may post

## 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 customers 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.<sup>13</sup>

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

Information on how Shopify handles cookies can be found in our Cookie Policy.<sup>14</sup>

## 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.<sup>15</sup>

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

---

<sup>12</sup>See: <https://www.shopify.com/legal/terms>.

<sup>13</sup>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.

<sup>14</sup>See: <https://www.shopify.ca/legal/cookies>.

<sup>15</sup>General Data Protection Regulation, Article 8. Individual member states may lower the age of consent.



# 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 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<sup>16</sup>

*Consent* of the data subject means the data subject has agreed to the processing of their personal data with a clear affirmative action.<sup>17</sup>

This agreement must be:

- Freely given
- Specific
- Informed
- Unambiguous

Merchants, as controllers of their customers' 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.<sup>18</sup>

As its merchants' processor, Shopify is not responsible for the merchants' legal bases but only processes customers' 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.

Upon request, Shopify will provide merchants with any reasonable information they require to obtain consent. Information on the cookies that Shopify places can be found in our Cookie Policy.<sup>19</sup>

## 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

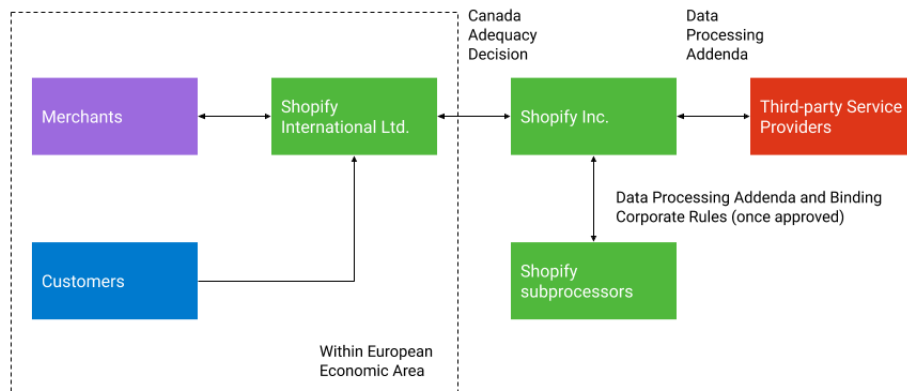
<sup>16</sup>General Data Protection Regulation, Article 6.

<sup>17</sup>General Data Protection Regulation, Article 4(11).

<sup>18</sup>General Data Protection Regulation, Article 7(1).

<sup>19</sup>See: <https://www.shopify.ca/legal/cookies>.

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.<sup>20</sup>

## 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 done through contractual data protection addenda (DPAs) with third-party service providers.

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.

<sup>20</sup>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>.

## 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 Customer 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 customers.

## Data subject rights

The GDPR provides data subjects (in this case, customers) with certain rights over their personal data. Generally, data subject requests must be addressed within one month, unless they are exceptionally complex or numerous.<sup>21</sup> The following rights are granted to data subjects.

### 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 customer to erase their personal data 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 navigate to the customer's page in their admin, and click "Remove Personal Data". This button is available to the Account Owner only.

After a request is received, Shopify will ensure that the relevant personal data is erased. Shopify will also send requests to the apps and channels that the merchant has installed to similarly redact that customer's data. 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.

Shopify will email the merchant once the redaction is complete. The merchant can then notify the customer.

### Timing

Once an erasure request is submitted, the merchant has a ten day grace period in which to cancel the request. To cancel the request, the merchant can email [privacy@shopify.com](mailto:privacy@shopify.com) and specify which customer's redaction request should be cancelled.

Personal data will not be erased from Shopify if the customer has made an order within the last 180 days (the usual window in which a customer can make a chargeback). However, Shopify will log the erasure request, and automatically erase the data once this time has passed. If a merchant wishes to override this 180 day hold, they may email [privacy@shopify.com](mailto:privacy@shopify.com) to waive the waiting period.

If the customer makes another purchase after their information has been redacted, a new customer account will be created.

<sup>21</sup>General Data Protection Regulation, Article 12(3).

## Scope

When processing a request for erasure, Shopify will anonymise the personal data of the customer, 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. Shopify will also not redact any text that has been entered manually by the merchant into free-form text boxes, such as comments on a customer's timeline or notes on orders. Merchants may edit or delete this text themselves at any time.

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 request the information from Shopify. Similar to a request for erasure, if a customer requests access to their personal data, the merchant should first validate the identity of the requester.

To submit a request, the merchant can navigate to the customer's page in their admin, and click "Send Customer Data".

When Shopify receives the request, it will:

- Confirm whether personal data about a customer is being processed by Shopify
- Confirm what categories of data are being processed by Shopify
- Provide the customer or merchant 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.<sup>22</sup>

Shopify's platform allows a merchant to change customer records directly from their store admin.<sup>23</sup>

## 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.<sup>24</sup> 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 customer 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.<sup>25</sup>

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

<sup>22</sup>General Data Protection Regulation, Article 16.

<sup>23</sup>However, current orders cannot be modified.

<sup>24</sup>General Data Protection Regulation, Article 21.

<sup>25</sup>General Data Protection Regulation, Article 25, 32.

# 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 customers using the HTTPS protocol.

Shopify also encrypts any sensitive stored information, and salts and hashes merchant and customer 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 customers
- 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.<sup>26</sup>

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

- Tier III
- ISO 27001
- PCI-DSS

---

<sup>26</sup>See: <https://www.shopify.ca/pci-compliant>.

# 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's annual Transparency Report can be found at the following link: <https://www.shopify.com/security/transparency-report>.