Shopify takes matters of privacy and data protection seriously, and we contractually commit to our merchants that we will comply with data protection laws such as the General Data Protection Regulation, Regulation (EU) 2016/679, (the "GDPR"). In order to do that, we have designed our infrastructure to transfer data across borders in compliance with the GDPR. In particular, we have structured our data flows such that all personal data about European data subjects is initially received and processed within Europe (specifically in Ireland). Shopify then transfers that data onwards to Canada and to other locations, as we explain in more detail in this whitepaper.

1 GDPR cross-border transfer requirements

When personal data of European residents is transferred out of Europe, the GDPR requires that data to be protected under specific mechanisms, including:

- **Law**: the privacy law of the 'destination' country is determined to be adequate to ensure the data is protected (Article 45). The European Commission has determined that Canada's private sector privacy law, which governs how Shopify's parent company processes data, adequately protects this data.

- **Treaty**: countries may enter into international treaties to allow the cross-border flow of personal data, such as the EU-U.S. Privacy Shield. The European Commission may decide any such treaty is adequate to ensure that data is protected (Article 50). However, the EU-U.S. Privacy Shield was invalidated by the Court of Justice for the European Union on July 16, 2020.

- **Contract**: personal data may be transferred between a European entity and a non-European entity under a contract with "Standard Contractual Clauses" ("SCCs"). The language of the SCCs is approved by the European Commission.

- **Policy**: personal data may be transferred within a group of companies (for example between Shopify Inc. and Shopify Payments (USA) Inc.) if the companies have an internal policy for protecting data called "Binding Corporate Rules" ("BCRs"), which are approved by a Data Protection Authority (Article 47). Shopify is in the process of having its BCRs approved.

2 Our data infrastructure

As explained in our GDPR Whitepaper, when you use Shopify’s services your contract includes a Data Processing Addendum between you and Shopify’s three entities that offer our services in different jurisdictions: Shopify Inc. (our parent company, located in Canada), Shopify International Ltd. (located in Ireland), and Shopify Commerce Singapore Pte. Ltd. (located in Singapore).

Per Section 2.1 of our Data Processing Addendum¹, when we receive data about a European data subject, that data is initially received from you and/or the data subject by Shopify International Ltd., in Ireland. While we cannot advise you on your obligations under data protection laws, in our view we process this personal data within Europe and Shopify International Ltd. is not importing this data outside of Europe initially.

In order to offer our global platform, Shopify International Ltd. then transfers this data to Shopify Inc., our parent company. To the extent that the GDPR applies to this transfer, this initial transfer from Ireland to Canada is conducted pursuant to Article 45 – a transfer on the basis of an adequacy decision. In this case, the transfer is to Shopify Inc., a Canadian company subject to Canada's Personal Information Protection and Electronic Documents Act ("PIPEDA"). Because this transfer is to a company subject to PIPEDA, it is conducted under the European Commission’s adequacy decision 2002/2/EC.

¹Please note that if you have a negotiated DPA, section numbers may differ and your negotiated agreement will apply.
Shopify Inc. then may use other subprocessors. These subprocessors are located around the world, and the specific subprocessors used will vary depending on specific circumstances (such as the location of your store, your store configuration, specific Shopify services you may use, the extent to which you use Shopify support, etc.). At present, we comply with the export requirements of Canadian privacy law.

In June 2021, the European Commission adopted new Standard Contractual Clauses. Shopify can confirm, for informational purposes only, that it is in discussions with subprocessors regarding executing the new Standard Contractual Clauses covering onward transfers from Canada to subprocessors located around the world. While Shopify is aiming to have the new Standard Contractual Clauses signed by its subprocessors as quickly as possible, Shopify is unable to provide an estimated timeframe for completion of this step.

Further, we are in the process of having Binding Corporate Rules approved, which will support transfers between Shopify’s entities (some of whom act as subprocessors for your customers’ personal data).

Note that when we transfer data to service providers in the United States, we **DO NOT** rely on the recently invalidated EU-U.S. Privacy Shield. Nor do we rely on SCCs. SCCs and the former Privacy Shield only apply to transfers from a European entity to a non-European entity (specifically an American entity in the case of the Privacy Shield), which does not apply to onwards transfers from Canada. Instead, we transfer this data pursuant to the requirements of PIPEDA (which the European Commission has determined is adequate), and subject to specific contractual agreements (again with provisions materially similar to those in our Data Processing Addendum with you).

The diagram below illustrates the flow of data of European residents, and how Shopify ensures protection each step of the way.

---

### Frequently asked questions

**Q:** Since Shopify is based in Canada, am I exporting data about my European customers to Canada when I use Shopify?

**A:** All personal data about European customers is initially received and processed by Shopify International Ltd., which is located in Ireland. Shopify International Ltd. then may export this data as explained above, and is responsible for compliance with GDPR export requirements when it does.

**Q:** Your Data Processing Addendum says that you may transfer personal data to the United States. Do you?

**A:** While the specific subprocessors we use will depend on the manner in which you use our service, our Canadian entity Shopify Inc. will almost certainly transfer and process some personal data of your...
customers using subprocessors in the United States. As explained in our Data Processing Addendum and above, we transfer this data in compliance with PIPEDA, and subject to strict contractual commitments.

Q: You participated in the EU-U.S. Privacy Shield – does the decision in Case C-311/18 invalidating the European Commission’s Decision 2016/1250 (“Schrems II”) affect how the personal data of my customers is transferred, since you can no longer rely on the Privacy Shield?

A: No. While we historically participated in the EU-U.S. Privacy Shield for some purposes, we have long relied on PIPEDA and contractual agreements with our subprocessors to transfer personal data from Canada to our subprocessors in the United States (as explained above). Schrems II’s invalidation of the Privacy Shield therefore does not affect how we transfer data to our subprocessors.

Q: Will you enter into Standard Contractual Clauses with us to govern our transfer of our customers’ data to you?

A: No. As explained above, we receive and initially process your customers’ personal data within Ireland. We therefore believe that we are not importing this personal data from you outside of Europe, and so SCCs are not appropriate.

Q: Do you enter into Standard Contractual Clauses with your subprocessors to govern your transfer of our customers’ data to them?

A: In June 2021, the European Commission adopted new Standard Contractual Clauses. Shopify can confirm, for informational purposes only, that it is in discussions with subprocessors regarding executing the new Standard Contractual Clauses covering onward transfers from Canada to subprocessors around the world. While Shopify is aiming to have the new Standard Contractual Clauses signed by its subprocessors as quickly as possible, Shopify is unable to provide an estimated timeframe for completion of this step.

Historically, Shopify did not enter into SCCs with its subprocessors. As the European Commission explains, legacy SCCs were only approved for transferring data from a data controller located in Europe to a data controller or data processor located outside of Europe. When Shopify Inc., a Canadian entity acting as a data processor for your customers’ data, transfers your customers’ personal data to our subprocessors, it is not a data controller located in Europe, and therefore cannot rely on such legacy SCCs. That said, as explained above and in Section 2.3 of our Data Processing Addendum, even if a transfer is not yet covered by the new SCCs, any transfer of your customers’ personal data to a subcontractor occurs subject to a contract that is materially similar to our Data Processing Addendum with you.

Q: Do you use any Supplementary Measures?

A: The Schrems II ruling requires companies to undertake data transfer risk assessments and, where appropriate, to implement “supplementary measures” in addition to any data export mechanisms they rely upon when transferring personal data to non-EEA countries. These supplementary measures, when used in conjunction with data export mechanisms, are intended to ensure that data processed outside of the EEA remains protected to a standard that is essentially equivalent with the GDPR.

While we believe that Shopify has implemented a data transfer regime that does guarantee an essentially equivalent level of protection, Shopify continues to maintain a data protection program that incorporates recommendations of the EDPB to give merchants further assurance of the security of their data. The three categories of recommended supplementary measures are: technical, contractual, and organizational.

Technical measures: - Shopify encrypts credit card information in transit and at rest, and is PCI compliant. - Shopify maintains a SOC 2 Type II and SOC 3 report². - Shopify conducts regular third-party penetration testing and vulnerability assessments. - Shopify participates in a bug-bounty program to receive security reports. - Employee access to Shopify infrastructure is controlled by a Single Sign-On

²SOC 2 Type II report available upon request under NDA.
(SSO) account with two-factor authentication required (2FA). - Shopify maintains employee internal access policies based on "least privilege". - Shopify provides merchants with the technical capability to honor all data subject requests. - All merchant personal data is redacted after account termination, unless we are legally required to retain information for a specified period of time.

**Contractual measures:** - In its contracts with its merchants, Shopify contractually commits to comply with all applicable data protection laws. - Shopify requires all vendors which receive personal data to agree to Data Protection Addenda which include comparable contractual commitments to those that Shopify guarantees its merchants. These DPA include requirements to use data only to provide the services, to not sell personal information, to report all data incidents within specified timelines, to implement reasonable security measures, to effect data subject rights, to object to compelled disclosure where possible or allow Shopify to object, and to delete all data upon termination of the contract.

**Organizational measures:** - Shopify publicly commits to object to any voluntary disclosure of data it holds, unless it is legally bound to produce information. When possible, Shopify commits to informing merchants of third party requests to access their data. - Shopify publishes an annual Transparency Report detailing when Shopify is legally required to produce information. - All Shopify employees receive privacy and security training. - Shopify incident response teams are on-call 24 hours a day. - All Shopify employees and contractors agree to confidentiality clauses in their employment contracts, and agree to abide by Shopify’s internal data protection policies. - Shopify maintains an internal Privacy Working Group which raises and resolves privacy issues across the organization. If needed, issues are escalated to a Privacy Committee and the Board of Directors. - Shopify does not knowingly disclose (or permit access to) the personal data it processes in a massive, disproportionate and indiscriminate manner to (or by) any governmental authority.

**Q:** Where is my data stored? Can I specify the country of storage?

**A:** We primarily store our merchant and customer data in the US and Canada. We cannot commit to storage in a specific jurisdiction. Shopify dynamically rebalances storage between multiple Google Cloud Platform regions in order to ensure that we can offer a reliable and scalable infrastructure that can handle unpredictable volumes across our entire merchant base. We need to be able to move data geographically in order to operate our service. Merchants need to assess how this affects their legal requirements, and use our service accordingly.