Data Processing Addendum

Version 1.0. Effective 18 October 2026.

This is a copy of the Data Processing Addendum between the merchant named below and Commit & Push Ltd, generated from the version published at https://commitandpush.io/privacy/dpa/. To sign it, fill in your details below and on the last page, sign, and email it to privacy@commitandpush.io. We will countersign and send you a copy.

The signed copy records the parties and does not change the terms published at commitandpush.io/privacy/dpa/, which apply from acceptance in the app.

Parties

Data exporter (you, the merchant)

Legal entity name	
Company number	
Registered address	
Contact name	
Contact email	
Role	Controller
Competent supervisory authority	

Data importer (us)

Legal entity name	Commit & Push Ltd
Company number	17515624 (England and Wales)
Registered address	71-75 Shelton Street, Covent Garden, London WC2H 9JQ, United Kingdom
Contact	Privacy team, privacy@commitandpush.io
Role	Processor
Supervisory authority	Information Commissioner's Office, registration ZC272983

EU representative	Prighter EU Rep GmbH, Schellinggasse 3/10, 1010 Vienna, Austria; online at https://app.prighter.com/portal/commit-and-push-ltd

Data Processing Addendum

About this addendum

> **In short:** When our apps handle your customers' personal data, we do it only for you and on your instructions. This addendum is the contract that says so. It applies automatically; you don't need to sign it.

This Data Processing Addendum ("Addendum") forms part of the agreement between you, the merchant who installs one of our apps ("you"), and Commit & Push Ltd (company number 17515624), trading as Commit & Push ("we", "us"), for the use of our Shopify apps, made up of our terms of service and the documents they include (the "Agreement"). It applies whenever we process Customer Personal Data (defined below) on your behalf, and it takes effect when you accept our terms in the app, before the app starts processing any Customer Personal Data.

If this Addendum conflicts with the rest of the Agreement, this Addendum applies to the processing of Customer Personal Data. If you need a signed copy for your records, download the PDF, fill in your details and email it to privacy@commitandpush.io.

Definitions

- **Data Protection Law** means all laws on privacy and personal data that apply to the processing, including the UK GDPR and the Data Protection Act 2018, the EU GDPR, the Swiss Federal Act on Data Protection, and US state privacy laws such as the California Consumer Privacy Act.
- **Customer Personal Data** means personal data about your store's customers that we process on your behalf through our apps, or when we help you with them, as described in Annex I.
- **Controller**, **processor**, **data subject**, **personal data breach** and **processing** have the meanings given in Data Protection Law. Under US state laws, "controller" includes "business" and "processor" includes "service provider".
- **Sub-processor** means a supplier we engage that processes Customer Personal Data.

Roles

For Customer Personal Data, you are the controller and we are your processor. You are responsible for having a lawful basis for the processing and for giving your customers the information the law requires, including in your own privacy policy. For personal data about you and your staff, we are a controller under our privacy policy, and this Addendum does not apply to it.

Our commitments

We will:

1. **Follow your instructions.** Process Customer Personal Data only to provide our apps you have installed in your store, as described in Annex I, and on your documented instructions. Your instructions are this Addendum, the Agreement, and your use and settings of the app. Approving the app's permissions in Shopify and accepting our terms in the app instructs us to sync the data it needs to work, as described in Annex I. We don't start syncing Customer Personal Data until you have accepted. We will tell you if we believe an instruction breaks Data Protection Law, unless the law prevents us.
2. **Keep it confidential.** Make sure anyone we authorise to process Customer Personal Data is bound by confidentiality.
3. **Keep it secure.** Apply the security measures in Annex II, and keep them appropriate to the risk.
4. **Use sub-processors carefully.** Use only the sub-processors on our sub-processor list, under written terms that protect Customer Personal Data at least as well as this Addendum. You give us general authorisation to use them. We will tell you at least 14 days before we add a new sub-processor to our list, or as soon as we reasonably can if the change is urgent for security or to keep the service running. Each supplier's own sub-processors are listed on its website, linked from our sub-processor list, and the supplier keeps that list up to date. If you object on reasonable data protection grounds, tell us in writing within 14 days of our notice and give your reasons. We will then work with you to find a solution; if we can't, you may stop using the affected app, and we will refund any fees you prepaid for the period after it stops. We remain responsible for our sub-processors.
5. **Help with requests.** Help you respond to your customers' requests to exercise their rights. Shopify's customer data request and erasure notices reach us automatically; we act on erasure notices within 30 days and provide requested data to you.
6. **Help with your obligations.** Give you reasonable help with security, breach notification, data protection impact assessments and consultations with regulators, taking into account the nature of the processing and the information available to us.
7. **Tell you about breaches.** Notify you without undue delay, and in any case within 48 hours, after becoming aware of a personal data breach affecting Customer Personal Data, with the information you need to meet your own obligations. We will email the account owner's address for your store that Shopify gives us, and any privacy contact you have given us, and show a notice in the app. The notice will describe the nature of the breach, the categories and approximate number of people and records affected, the likely consequences, the measures we have taken or propose to take, and who to contact for more information. If we don't know everything at first, we will send what we know and update you as the facts emerge. We also notify Shopify within 24 hours where Shopify's terms require it.
8. **Delete it at the end.** When you uninstall an app, delete Customer Personal Data within 30 days of Shopify's erasure notice, which Shopify sends 48 hours after you uninstall, unless

the law requires us to keep it or another of our apps installed in your store still uses it. Database backups containing it are deleted within a further 30 days, and error reports and failed Shopify notifications, which can occasionally contain it, within 90 days of being created. Because Shopify holds the original data, we do not return copies unless you ask before uninstalling. If you ask, we will confirm in writing once deletion is complete.

9. **Show we comply.** Make available the information reasonably needed to show that we meet this Addendum, answering your questions in writing and sharing our policies and our suppliers' security reports. If that is not enough, allow an audit by you or an independent auditor bound by confidentiality, on at least 30 days' notice, no more than once a year, at your cost, unless a regulator requires otherwise or there has been a breach affecting your data. Audits are carried out remotely by document review and interviews, cover only how we process your Customer Personal Data, and never give access to other merchants' data or to our systems in a way that could affect their security.
10. **Not misuse it.** Not sell or share Customer Personal Data, not use it for any purpose other than providing our apps to you (including our own marketing or training AI models), not combine it with personal data from other sources except as needed to provide our apps, and not contact your customers. We may create statistics that don't identify any person, store or merchant, such as error rates and performance figures, only to run, secure and fix the app you installed; we never sell or share them, publish them, use them for another app or use them to train AI.

International transfers

We may transfer Customer Personal Data to countries outside the UK, the European Economic Area and Switzerland, including the United States, as described on our sub-processor list. Where the law requires a transfer safeguard:

- for transfers from the EEA, the European Commission's Standard Contractual Clauses (Decision 2021/914) are incorporated into this Addendum. Module 2 (controller to processor) applies where you are a controller, and Module 3 (processor to processor) where you are yourself a processor acting for someone else. Clause 7 (docking) is included, option 2 of Clause 9 applies (general authorisation, with the notice period in this Addendum), the optional wording in Clause 11 is omitted, Irish law governs under Clause 17, and the courts of Ireland have jurisdiction under Clause 18;
- for transfers from the UK, the International Data Transfer Addendum issued by the Information Commissioner under section 119A of the Data Protection Act 2018 applies, with its tables completed using the information in this Addendum, and neither party may end it under its Section 19;
- for transfers from Switzerland, the Standard Contractual Clauses apply with the changes the Swiss Federal Data Protection and Information Commissioner requires, with that Commissioner as the competent authority.

The European Union recognises the UK as giving adequate protection, so Customer Personal

Data can come to us from the EEA without further safeguards. The Standard Contractual Clauses (Module 2 or 3, as applicable) cover its onward transfer to our sub-processors in the United States.

Where a sub-processor is certified under the EU-US Data Privacy Framework, its UK Extension or the Swiss-US Data Privacy Framework, we may also rely on that certification.

The clauses need some details filled in. This table shows where each one is in this Addendum.

What the clauses need	Where it is
SCC Annex I.A: list of parties	Annex I, "Parties"
SCC Annex I.B: description of the transfer	Annex I
SCC Annex I.C: competent supervisory authority	Annex I, "Competent supervisory authority"
SCC Annex II: technical and organisational measures	Annex II
SCC Annex III: list of sub-processors	Annex III and our sub-processor list
UK Addendum Table 1: parties	Annex I, "Parties"
UK Addendum Table 2: selected clauses and options	This section
UK Addendum Table 3: appendix information	Annexes I, II and III
UK Addendum Table 4: ending the Addendum	This section: neither party may end it

Requests from public authorities

If a court, regulator, law enforcement body or other public authority asks us to disclose Customer Personal Data, we will:

- disclose it only if the law requires us to;
- check that the request is valid and that the authority has the power to make it;
- challenge a request that is too broad, where we have reasonable grounds to do so;
- disclose only the minimum the request requires;
- tell you before we disclose anything, unless the law forbids it; and
- keep a record of the request and of what we did.

US state privacy laws

Where US state privacy laws apply, we act as your service provider or processor. We will not sell or share Customer Personal Data, retain, use or disclose it outside our direct business

relationship with you or for any purpose other than providing the app, or combine it with other personal data except as those laws allow. We will comply with those laws, give the same level of privacy protection they require, and tell you if we can no longer meet our obligations. You may take reasonable steps to stop and fix any unauthorised use.

Liability and duration

Each party's liability under this Addendum is subject to the limits and exclusions in the Agreement, except where the law does not allow them to apply. This Addendum lasts for as long as we process Customer Personal Data for you, and the commitments on deletion and confidentiality continue after that.

We may update this Addendum to reflect changes in the law or our services. We will not reduce the protection it gives Customer Personal Data, and we will tell you about material changes at least 30 days in advance, by email and in the app, as our terms describe in Changes to these terms. The updated Addendum applies from the date in our notice. If you don't agree with a change, you can stop using the app and uninstall it before then.

Annex I: Details of the processing

Item	Detail
Parties	You, as controller (the data exporter), and Commit & Push Ltd (company number 17515624), 71-75 Shelton Street, Covent Garden, London WC2H 9JQ, United Kingdom, as processor (the data importer). Contact: privacy@commitandpush.io. EU representative: Prighter EU Rep GmbH, Schellinggasse 3/10, 1010 Vienna, Austria
Subject matter	Providing our Shopify apps you have installed in your store, and support for them
Duration	While our apps are installed in your store; data another of our installed apps still uses is kept until that app is uninstalled too. After Shopify's erasure notice, we delete the data within 30 days, and database backups containing it within a further 30 days. Error reports and failed Shopify notifications, which can occasionally contain Customer Personal Data, are kept for up to 90 days. Background job history is kept for 7 days. Support access to your store lasts until you remove it, and ends automatically after 90 days unused

Item	Detail
Nature and purpose	Storing, organising, analysing and deleting data so the app can work for you, as described on each app's privacy page. When you ask for help, viewing the data you share with us or let us see in your store, for example through a Shopify collaborator account, only to resolve your request (see Support and access to your store)
Data subjects	Your store's customers
Categories of data	For Discount Magic: Shopify customer ID, name, email address, phone number, customer segment membership, and order details (order number, discounts used, amounts, country, language, marketing source and notes added at checkout). When you ask for help: the customer and order details you share with us or let us see in your store
Special categories	None intended. Free-text fields you or your customers fill in could contain anything, so please don't put sensitive data in them
Frequency	Continuous while the app is installed
Location of processing	Stored in the United States. See Where your data is and our sub-processor list
Sub-processors	As listed on our sub-processor list
Competent supervisory authority	The authority competent for you under the EU GDPR; for UK transfers, the Information Commissioner's Office

Annex II: Security measures

- **Encryption.** Data is encrypted in transit with TLS and at rest by our hosting and database providers. Access tokens for Shopify and connected services are additionally encrypted by us.
- **Access control.** Production access is limited to the people who need it, uses individual accounts with multi-factor authentication, and is logged. Operational database access uses a role that hides customer personal data.
- **Separation.** Development and test environments use synthetic data, never Customer Personal Data. Each store's data is kept separate within our systems.
- **Minimisation.** We request only the Shopify data the app needs, keep personal data out of logs and analytics where we can, and delete temporary files on short timers.
- **Resilience.** Managed hosting across multiple zones, daily encrypted database backups kept for 30 days in the United States, and monitoring and alerting.

- **Secure development.** Code review before release, dependency updates, automated security checks, and secrets kept in a managed secret store.
- **Incident response.** A documented process for detecting, containing, investigating and notifying personal data breaches.
- **People.** Production access is limited to the people who need it to run our services, all bound by confidentiality terms. We review access whenever someone joins or leaves, and at least once a year.
- **Suppliers.** Sub-processors are chosen for their security and bound by written data protection terms.

Annex III: Sub-processors

Our current sub-processors, what they do, where they process data and the safeguards for each are on our sub-processor list, which forms part of this Addendum. Suppliers shown there with "No" for your customers' data don't process Customer Personal Data; we list them so the page covers everyone who handles personal data for us.

Signatures

Signed for each party by a person authorised to sign for it. The signed copy records the parties and does not change the terms published at commitandpush.io/privacy/dpa/, which apply from acceptance in the app.

For the data exporter (the merchant)

Name	
Job title	
Signature	
Date	

For the data importer (Commit & Push Ltd)

Name	
Job title	
Signature	
Date	