Shopify

Binding Corporate Rules:

Controller Policy

Contents

Part I: Introduction

This Binding Corporate Rules: Controller Policy ("**Controller Policy**") applies when Shopify processes personal data as a controller and transfers personal data between group members. This Controller Policy applies regardless of whether our group members process personal data by manual or automated means.

This Controller Policy applies to transfers of personal data (i) from a group member in Europe to a group member in a third country; and (ii) from a group member in a third country to another group member in a third country, where such personal data falls within the scope of the GDPR in accordance with the extra-territorial scope of the GDPR provided for in Article 3(2) GDPR.

For an explanation of some of the terms used in this Controller Policy, like "controller", "processor", and "personal data", please see the section titled "Important terms used in this Controller Policy" below.

Types of personal data within the scope of this Controller Policy

This Controller Policy applies to all personal data that we process as a controller, including personal data processed in the course of our business activities, employment administration and vendor management – such as:

- **Human resources data:** personal data of past and current employees, individual consultants, independent contractors, temporary staff and job applicants;
- **Merchant data:** personal data relating to representatives of merchants who use our business services;
- **Partner data:** personal data relating to Shopify partners and app developers who provide services or develop technology for merchants in connection with their use of Shopify's technology;
- **Customer data**: personal data relating to end users of Shopify's customer-facing applications and services (including, for example, Shopify's corporate website, other

online properties, Shop Pay, or Shop App) and personal data relating to merchant customers for the development and provision of Enhanced Services, as described in Appendix 12; and

- **Vendor data:** including personal data of individual contractors and of account managers and staff of third parties who provide services to us.

Further information on the types of personal data that we process as a controller is contained in **Appendix 12**.

Our collective responsibility to comply with this Controller Policy

All group members and their staff must comply with, and respect, this Controller Policy when processing personal data as a controller, irrespective of the country in which they are located.

In particular, all group members who process personal data as a controller must comply with:

- the rules set out in **Part II** of this Controller Policy;
- the practical commitments set out in **Part III** of this Controller Policy;
- the third party beneficiary rights set out in **Part IV** of this Controller Policy; and
- the policies and procedures appended in **Part V** of this Controller Policy.

Management commitment and consequences of non-compliance

Shopify's management is fully committed to ensuring that all group members and their staff comply with this Controller Policy at all times.

Non-compliance may cause Shopify to be subject to sanctions imposed by competent supervisory authorities and courts, and may cause harm or distress to data subjects whose personal data has not been protected in accordance with the standards described in this Controller Policy.

In recognition of the gravity of these risks, staff members who do not comply with this Controller Policy may be subject to disciplinary action, up to and including dismissal.

Relationship with Shopify's Binding Corporate Rules: Processor Policy

This Controller Policy applies only to personal data that Shopify processes as a controller (i.e. for its own purposes). Shopify has a separate Binding Corporate Rules: Processor Policy ("**Processor Policy**") that applies when it processes personal data as a processor in order to provide a service to a third party (such as a merchant). When a Shopify group member processes personal data as a processor to provide its services, it must comply with the Processor Policy.

In some situations, group members may act as both a controller and a processor. Where this is the case, they must comply both with this Controller Policy and also the Processor Policy as appropriate. If in any doubt as to which policy applies to you, please speak with Shopify's Data Protection Team whose contact details are provided below.

Where will this Controller Policy be made available?

This Controller Policy is accessible on Shopify's corporate website at www.shopify.com/legal.

Important terms used in this Controller Policy

For the purposes of this Controller Policy:

- the term **applicable data protection laws** means any data protection laws applicable to the processing of the personal data in question, including the data protection laws in force in the territory from which a group member initially transfers personal data under this Controller Policy. Where a European group member transfers personal data under this Controller Policy to a non-European group member, the term applicable data protection laws shall include the European data protection laws applicable to that European group member (including the General Data Protection Regulation (as defined below));

- the term **binding corporate rules** or **BCRs** means this set of Binding Corporate Rules for Controllers and the Appendices which are applicable and binding on each group member;

- the term **consent** means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to them;

- the term **controller** means the natural or legal person which, alone or jointly with others, determines the purposes and means of the processing of personal data. For example, Shopify is a controller of its human resources data and merchant data;

- the term **data exporter** means the group member exporting personal data or otherwise making personal data available to the data importer;

- the term **data importer** means the group member outside Europe that receives or otherwise has access to personal data from the data exporter;

- the term **data subject** means a natural person who is the subject of personal data;

- the term **Europe** and **European** as used in this Policy refers to the countries in the European Economic Area and Switzerland;

- the term **European data protection law** means the GDPR and any data protection laws of a European country, including local legislation implementing the requirements of the GDPR or equivalent laws and subordinate legislation, in each case as amended from time to time;

- the term **General Data Protection Regulation** or **GDPR** means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the Processing of Personal Data and on the free movement of such data and repealing Directive 95/46/EC;

- the term **group member** means the members of Shopify's group of companies listed in **Appendix 1**;

- the term **lead supervisory authority** means the lead supervisory authority for Shopify's BCRs, being the Irish Data Protection Commission;

- the term **personal data** means any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

- the term **processing** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

- the term **processor** means a natural or legal person which processes personal data on behalf of a controller (for example, a third party service provider that is processing personal data in order to provide a service to Shopify);

- the term **special categories of personal data** means information that relates to a data subject's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, or data concerning a natural person's sex life or sexual orientation. It also includes information about a data subject's criminal offences or convictions, as well as any other information deemed sensitive under applicable data protection laws;

- the term **staff** refers to all employees, new hires, individual contractors and consultants, and temporary staff engaged by any Shopify group member. All staff must comply with this Controller Policy;

- the term **supervisory authority** means an independent public authority which is established by a European country to be responsible for monitoring the application of European data protection law, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the EU;

- the term **transfer** means a transfer of personal data which undergoes processing or is intended for processing after transfer to a third country or to an international organisation including onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation;

- the term **third country** means any country outside Europe; and

- the term **we** or **our** refers to the Shopify group of entities.

How to raise questions or concerns

If you have any questions regarding this Controller Policy, your rights under this Controller Policy or applicable data protection laws, or any other data protection issues, you can contact Shopify's Data Protection Team using the details below. Shopify's Data Protection Team will

either deal with the matter directly or forward it to the appropriate person or department within Shopify to respond, within 7 business days of receipt of the request.

Attention: Data Protection Team

Email: privacyoffice@shopify.com

Address:

Shopify Data Protection Officer
c/o Intertrust Ireland
2nd Floor 1-2 Victoria Buildings
Haddington Road
Dublin 4, D04 XN32
Ireland

Shopify's Data Protection Team is responsible for ensuring that changes to this Controller Policy are notified to the group members and to data subjects whose personal data is processed by Shopify in accordance with **Appendix 9**.

If you want to exercise any of your data protection rights, please see the data protection rights procedure set out in **Appendix 3**. Alternatively, if you are unhappy about the way in which Shopify has used your personal data, you can raise a complaint in accordance with our complaint handling procedure set out in **Appendix 7**.

Part II: Our obligations

This Controller Policy applies in all situations where a group member processes personal data as a controller anywhere in the world. All staff and group members must comply with the following obligations:

Rule 1 – Lawfulness: ***We must ensure that all processing complies with applicable data protection laws and this Controller Policy.***	We must at all times comply with applicable data protection laws, as well as the standards set out in this Controller Policy, when processing personal data. As such: ● where applicable data protection laws exceed the standards set out in this Controller Policy, we must comply with those laws; but ● where there are no applicable data protection laws, or where applicable data protection laws do not meet the standards set out in this Controller Policy, we must process personal data in accordance with the standards set out in this Controller Policy. We have provided a list of legal bases for processing which the group members intend to rely on in **Appendix 13**.
Rule 2 – Fairness and transparency: ***We must inform data subjects how and why their personal data will be processed.***	We must provide data subjects with the Fair Information Disclosures (see **Appendix 2**) when we process their personal data. We must take appropriate measures to communicate the Fair Information Disclosures to data subjects in a concise, transparent, intelligible and easily accessible form, using

	clear and plain language. The Fair Information Disclosures shall be provided in writing, or by other means, including, where appropriate, by electronic means. They may be provided orally, at the request of a data subject, provided that the identity of that data subject is proven by other means. In certain limited cases we may not need to provide the Fair Information Disclosures, as explained in **Appendix 2**. Where this is the case, the Data Protection Team must be informed and will decide what course of action is appropriate to protect the data subject's rights, freedoms and legitimate interests.
Rule 3 – Purpose limitation: ***We must process personal data only for specified, explicit and legitimate purposes and not further process that information in a manner that is incompatible with those purposes.***	We must only process personal data for specified, explicit and legitimate purposes that have been communicated to the data subjects concerned in accordance with **Rule 2** – Fairness and transparency. We must not process their personal data in a way that is incompatible with those purposes, except in accordance with applicable law which constitutes a necessary and proportionate measure in a democratic society or with the data subject's consent. In such cases, we must also provide the data subject with Fair Information Disclosures about the further processing in accordance with **Rule 2** – Fairness and transparency.

	In assessing whether any processing is compatible with the purpose for which the personal data was originally collected, we must take into account: ● any link between the purposes for which the personal data was originally collected and the purposes of the intended further processing; ● the context in which the personal data was collected, and in particular the reasonable expectations of the data subjects whose personal data will be processed; ● the nature of the personal data, in particular whether such data may constitute special categories of personal data; ● the possible consequences of the intended further processing for the data subjects concerned; and ● the existence of any appropriate safeguards that we have implemented in both the original and intended further processing operations.
Rule 4 – Data minimization ***We must only process personal data that is adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.***	We must only process personal data that is adequate, relevant and limited in order to properly fulfil the desired processing purposes. We must not process personal data that is unnecessary to achieve those purposes.

Rule 5 – Accuracy: ***We must keep personal data accurate and, where necessary, up to date.***	We must take appropriate measures to ensure that the data we process is accurate and, where necessary, kept up to date – for example, by giving data subjects the ability to inform us when their personal data has changed or become inaccurate. We must take every reasonable step to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
Rule 6 – Storage limitation: ***We will only keep personal data for as long as is necessary for the purposes for which it is collected and further processed.***	We must not keep personal data in a form which permits identification of data subjects for longer than is necessary for the purposes for which that data is processed. In particular, we must comply with Shopify's record retention policies.
Rule 7 – Security, integrity and confidentiality: ***We must implement appropriate technical and organisational measures to ensure a level of security of personal data that is appropriate based on the risks to the rights and freedoms of the data subjects.***	We must implement appropriate technical and organisational measures to: (i) ensure and to be able to demonstrate that processing is performed in accordance with the Controller Policy; and (ii) ensure a level of security appropriate to the risks to the rights and freedoms of data subjects and to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where processing involves transmission of personal data over a network, and against all other unlawful forms of processing.

	Such measures will ensure a level of security appropriate to the risk and may include as appropriate: ● the pseudonymisation and encryption of personal data; ● the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; ● the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and ● a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing. In particular, we must comply with the requirements in the security policies in place within Shopify, as revised and updated from time to time, together with any other security procedures relevant to a business area or function. We must ensure that any staff member who has access to or is involved in the processing of personal data does so only on instructions from Shopify and under a duty of confidence.
Rule 8 – Service provider management:	Where we appoint a service provider to process personal data on our behalf (i.e. a processor), we must: (1) engage only service providers providing sufficient guarantees to

We must ensure that our service providers also adopt appropriate security measures when processing personal data.	implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of applicable data protection laws, and (2) impose strict contractual terms on the service provider that require it: ● to act only on our instructions when processing that information, including with regard to transfers of personal data; ● to ensure that any of its staff who have access to the data are subject to a duty of confidence; ● to have in place appropriate technical and organisational security measures to safeguard the personal data; ● only to engage a sub-processor if we have given our prior specific or general written authorisation, and on condition the sub-processor agreement protects the personal data to the same standard required of the service provider; ● to assist us in ensuring compliance with our obligations as a controller under applicable data protection laws, in particular with respect to reporting data security incidents under **Rule 9** – Security Incident Reporting and responding to requests from data subjects to exercise their data protection rights under **Rule 10 –** Honouring data subjects' data protection rights. ● to return or delete the personal data once it has completed its services (or following termination for any reason); and

	● to make available to us all information we may need in order to ensure its compliance with these obligations and to allow for and to contribute to audits, including inspections.
Rule 9 – Security Incident Reporting: ***We must comply with any data security incident reporting requirements that exist under applicable law.***	Where we become aware of an incident that might present a risk to the personal data for which we are a controller, we will promptly notify the Data Protection Team. Any notifications to the Data Protection Team shall be deemed to be notifications to Shopify International Limited. The Data Protection Team will review the nature and seriousness of the data security incident and determine whether it is necessary under applicable data protection laws to notify competent supervisory authorities and/or data subjects affected by the incident. The Data Protection Team shall: ● if the data security incident is likely to result in a risk to the rights and freedoms to individuals whose personal data were affected by the incident, notify competent supervisory authorities without undue delay and, where feasible, within 72 hours, in accordance with applicable data protection laws. ● if the data security incident is likely to result in a high risk to individuals whose personal data were affected by the incident, notify those individuals without undue delay in accordance with applicable data protection laws. The Data Protection Team shall be responsible for ensuring that any such notifications, where necessary, are made

	without undue delay and not later than required by the applicable data protection laws. Such notifications to the supervisory authority shall be made in accordance with applicable data protection law and documented as required. Where the notification to the supervisory authority is not made within 72 hours after having become aware of the data security incident as required by Article 33 of the GDPR, it shall be accompanied by reasons for the delay. The Data Protection Team will document any personal data breach (comprising the facts relating to the personal data breach, its effects, and the remedial action taken), and the documentation should be made available to the competent supervisory authority upon request.
Rule 10 – Honouring data subjects' data protection rights: ***We must enable data subjects to exercise their data protection rights in accordance with applicable data protection laws.***	Various data protection laws around the world, including in Europe, provide data subjects with certain data protection rights, as detailed below. ● *The right to access:* This is a right for a data subject to obtain confirmation whether we process personal data about them and, if so, to be provided with details of that personal data and access to it. ● *The right to rectification:* This is a right for a data subject to obtain from us without undue delay the rectification of any inaccurate or incomplete personal data we may process about them. The data subject also has the right to have incomplete personal data completed, including by means of providing a supplementary statement.

	● *The right to erasure:* This is a right for a data subject to obtain from us the erasure of personal data about them on certain grounds – for example, where the personal data is no longer necessary to fulfill the purposes for which it was collected. ● *The right to restriction:* This is a right for a data subject to obtain from us restriction of processing of personal data about them on certain grounds. ● *The right to data portability:* This is a right for a data subject to receive personal data concerning them from us in a structured, commonly used and machine-readable format and to transmit that data to another controller, if certain grounds apply. ● *The right to object:* This is a right for a data subject to object, on grounds relating to his or her particular situation, to processing of personal data about them, if certain grounds apply. Where a data subject wishes to exercise any of their data protection rights, we must respect those rights in accordance with applicable law by following the Data Protection Rights Procedure (see **Appendix 3**).
Rule 11 – Ensuring adequate protection for transfers: ***We must not transfer personal data without ensuring adequate protection for the data in***	Various data protection laws around the world, including European data protection laws, prohibit transfers of personal data to third countries unless appropriate safeguards are implemented to ensure the transferred data

accordance with applicable data protection laws.	remains protected to the standard required in the country or region from which it is transferred. Where these requirements exist, we must comply with them. Whenever transferring personal data, the Data Protection Team must be consulted so that they can ensure appropriate safeguards have been implemented to protect the personal data being transferred. This includes when a group member who has received personal data pursuant to this Controller Policy intends to onward transfer that personal data to processors and/or controllers that are not bound by the Controller Policy. Any such personal data that have been transferred under this Controller Policy may only be onward transferred outside Europe to processors and controllers which are not bound by the Controller Policy if appropriate safeguards are implemented to ensure the transferred personal data remains protected to the standard required under GDPR. Appropriate safeguards may include: i) standard data protection clauses (i.e., the Standard Contractual Clauses) adopted by the European Commission, ii) standard data protection clauses adopted by a supervisory authority and approved by the European Commission, iii) an approved code of conduct together with binding and enforceable commitments of the recipient to apply the appropriate safeguards, including as regards data subjects' rights, or iv) an approved certification mechanism together with binding and enforceable commitments of the recipient to apply the

	appropriate safeguards, including as regards data subjects' rights. In the absence of an adequacy decision or appropriate safeguards, the transfer may take place only if one of the following conditions applies: i) the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the individual due to the absence of an adequacy decision and appropriate safeguards, ii) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request, iii) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person, iv) the transfer is necessary for important reasons of public interest laid down by applicable law, v) the transfer is necessary for the establishment, exercise, or defence of legal claims, vi) the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent, or vii) the transfer is made from a register that, according to applicable law, is intended to provide information to the public and is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by applicable law for consultation are fulfilled in the particular case.

	Before a group member can rely on this Controller Policy for a transfer of personal data to a third country the group member engaged in the processing that requires a transfer of personal data outside of Europe shall ensure that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the group member importing the data (including any requirements to disclose personal data or measures authorizing access by public authorities) prevent the group member importing the data from fulfilling its obligations under this Controller Policy. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society are not in contradiction with this Controller Policy. The group member shall in providing this assurance take into account the following elements as part of a transfer risk assessment: ● the specific circumstances of the transfer and of any envisaged onward transfers within the same third country or to another third country, including: o the type of recipients; o economic sector in which the transfer occurs; o the purpose of processing; o the categories and format of the personal data; o the location of the processing, including storage; and o the transmission channels used.

	● the laws of the country in which the group member is established in light of the circumstances of the transfer, including those requiring to disclose data to public authorities or authorising access by such authorities, as well as the applicable limitations and safeguards; and ● any safeguards in addition to those under the Controller Policy, including the technical and organisational measures applied during transmission and to the processing of the personal data in the country of destination in which the group member is established. The group member importing the data shall ensure that, in carrying out this assessment, it has used best efforts to provide the group member exporting the data with relevant information and agrees that it will continue to cooperate with the group member exporting the data in ensuring compliance with this Controller Policy. The group members involved in the transfer agree to document this assessment, as well as any supplementary measures adopted and make it available to any competent supervisory authority on request. The group member importing the data agrees to notify the group member exporting the data promptly if, after having commenced transfers of data pursuant to this Controller Policy, it has reason to believe that it is or has become subject to laws or practices that mean an essentially equivalent level of data protection as provided under this

	Controller Policy cannot be adhered to and more specifically that the requirements contained in this Controller Policy cannot be respected, including following a change in the laws of the third country of destination or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements contained in the Controller Policy. The group member importing the data shall also notify the DPO and Shopify International Limited of this fact. Following such notification to the group member exporting the data, or if the group member exporting data otherwise has reason to believe that the group member importing the data can no longer fulfil its obligations under this Controller Policy, the group member exporting the data shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the group members involved in the data transfer to address the situation. The Data Protection Team and Shopify International Limited will be involved in this assessment. The group member exporting the data shall suspend the transfer of personal data if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. Following such a suspension, the group member acting as data exporter will end the transfer to the relevant data importer if the Controller Policy cannot be complied with

	and compliance with the Controller Policy is not restored within one month of suspension, in line with **commitment 12 and 13** of Part III. The Data Protection Team will inform relevant group members of the assessment carried out and the results of that assessment for the purposes of identifying supplementary measures that might need to be put in place (in case the same type of transfer is carried out by any other group member) or when relevant transfers or categories of transfers may be suspended or ended. Group members exporting personal data pursuant to the Controller Policy will monitor developments in the third countries to which the data exporters have transferred personal data that could affect the initial assessment of the level of protection and the decisions taken accordingly on such transfers.
Rule 12 – Special Categories of Personal Data: ***We must only process special categories of personal data collected in Europe where we have obtained the data subject's explicit consent, unless there is an alternative legitimate basis for processing consistent with applicable data protection law.***	We will assess whether any special category of personal data is required for the intended purpose of processing before collecting it. In principle, we must obtain the data subject's explicit consent to collect and process his or her special categories of personal data, unless we are required by applicable law to collect and/or process such special categories of personal data or have another legitimate basis for such collection and/or processing consistent with the applicable law of the country in which the personal data was collected.

	Examples of such legitimate bases are where: ● processing is necessary in the field of employment and social security and social protection law; ● processing is necessary to protect the vital interests of the individual where the data subject is physically or legally incapable of giving consent; ● processing relates to personal data which are manifestly made public by the data subject; ● processing is necessary for the establishment, exercise or defence of legal claims; and ● processing is necessary for reasons of substantial public interest on the basis of applicable European law. When obtaining a data subject's consent, that consent must be given freely, and must be specific, informed and unambiguous.
Rule 13 – Direct marketing: ***We must allow data subjects to opt-out of receiving marketing information.***	All data subjects have the right to object, free of charge, to the use of their personal data for direct marketing purposes and we will honour all such opt-out requests.
Rule 14 – Automated decision-making, including profiling: ***We must respect data subjects' rights not to be subject to a***	We will not make any decision, which produces legal effects concerning a data subject or that similarly significantly affects them, based solely on the automated processing of that individual's personal data, including profiling, unless such decision is:

decision based solely on automated processing, including profiling, that produces legal effects or similarly significantly affects them.	● necessary for entering into, or performing, a contract between a group member and that data subject; ● authorized by applicable law (which, in the case of personal data transferred from Europe, must be European data protection law or applicable national law); or ● based on the data subject's explicit consent. In the first and third cases above, we must implement suitable measures to protect the data subject's rights and freedoms and legitimate interests, including the right to human intervention, and to express their view and to contest the decision. We must never make automated individual decisions about data subjects using their special categories of personal data unless they have given explicit consent under **Rule 12** or another lawful basis applies.

Part III: Compliance in practice

To ensure we follow the rules set out in this Controller Policy, in particular the obligations set out in Part II, Shopify and all of its group members must also comply with the following practical commitments:

1. Resourcing and compliance: ***We must have appropriate staff and support to ensure and oversee privacy compliance throughout the business.***	We have appointed a Data Protection Team to oversee and ensure compliance with this Controller Policy. The Data Protection Team will work with other relevant teams to oversee and enable compliance with this Controller Policy on a day-to-day basis. We have also appointed a Privacy Working Group. A summary of the roles and responsibilities of these teams is set out in our Privacy Compliance Structure at **Appendix 4**.
2. Privacy training: ***We must ensure staff are educated about the need to protect personal data in accordance with this Controller Policy.***	We must provide appropriate and up to date privacy training to staff members who: ● have permanent or regular access to personal data; or ● are involved in the processing of personal data or in the development of tools used to process personal data. We will provide such training in accordance with the Privacy Training Program (see **Appendix 5**).
3. Records of Data Processing: ***We must maintain records of the***	We must maintain a record of the processing activities that we conduct on all personal data transferred under this Controller Policy, in accordance with applicable data

data processing activities under our responsibility.	protection laws. These records should be kept in writing (which may include electronic form) and we must make these records available to competent supervisory authorities upon request. These records shall contain the following information: (i) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the Data Protection Officer ("DPO"); (ii) the purposes of the processing; (iii) a description of the categories of data subjects and of the categories of personal data; (iv) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations; (v) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1) of the GDPR, the documentation of suitable safeguards; (vi) where possible, the envisaged time limits for erasure of the different categories of data; and (vii) where possible, a general description of the technical and organisational security measures referred to in Article 32(1) of the GDPR. The Data Protection Team is responsible for ensuring that such records are maintained.
4. Audit: ***We must conduct data***	We will conduct data protection audits to verify compliance with all aspects of this Controller Policy by group members (including methods and action plans

protection audits on a regular basis.	ensuring that corrective actions have been implemented) on an annual basis, which may be conducted by either internal or accredited external auditors. In addition, we will conduct data protection audits on specific request from the DPO, or the board of directors of Shopify International Limited. We will also conduct data protection audits if there are indications of non-compliance to ensure verification of compliance with the Controller Policy. After each audit, the data protection audit reports will be submitted to the DPO, the board of directors of Shopify International Limited, and where appropriate, to Shopify's ultimate parent board. If non-compliance is identified through an audit, by a supervisory authority or otherwise, the group member shall rectify the identified non-compliance without delay. Such non-compliance shall be notified to the DPO, and where appropriate to the board of Shopify International Limited, and potentially, to Shopify's ultimate parent's board depending on the nature of the issue. The DPO will be kept informed of resolution measures, will oversee resolution measures and will direct any suspension and resumption of data transfers to that group member. If non-compliance persists and is not resolved without undue delay, then the DPO shall remove the group member from the Controller Policy and the DPO will notify the lead supervisory authority in the annual update. Shopify agrees that competent supervisory authorities can have access to the results of an audit on request.

	We will conduct any such audits in accordance with the Audit Protocol (see **Appendix 6**).
5. Data Protection Impact Assessments ***We must carry out data protection impact assessments where processing is likely to result in a high risk to rights and freedoms of data subjects, and to consult with competent supervisory authorities where required by applicable data protection laws.***	Where required by applicable data protection laws, we must carry out data protection impact assessments (DPIAs) whenever the processing of personal data transferred under this Controller Policy, particularly using new technologies, is likely to result in a high risk to the rights and freedoms of data subjects. In such instances, Shopify will carry out a DPIA prior to processing which will contain at least the following: ● a systematic description of the envisaged processing operations and the purposes of the processing; ● an assessment of the necessity and proportionality of the processing operations in relation to the purposes; ● an assessment of the risks to the privacy rights of data subjects; and ● the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and demonstrate compliance with applicable data protection laws. Where the DPIA indicates that the processing would still result in a high risk to data subjects, Shopify will consult with local supervisory authorities where required by

	applicable data protection laws.
6. Data protection by design and by default ***We must apply the principles of data protection by design and by default when designing and implementing new products and systems.***	When designing and implementing new products and systems which process personal data, we must apply the principles of data protection by design and by default. This means we must implement appropriate technical and organisational measures that: ● are designed to implement the data protection principles in an effective manner and to integrate the necessary safeguards in order to protect the rights of data subjects and meet the requirements of applicable data protection laws ("**data protection by design**"); and ● ensure that, by default, only personal data which are necessary for each specific processing purpose are collected, stored, processed and are accessible; in particular, that by default personal data is not made accessible to an indefinite number of people without the data subject's intervention ("**data protection by default**").
7. Complaint handling: ***We must enable data subjects to raise data protection complaints and concerns.***	We must enable data subjects to raise data protection complaints and concerns (including complaints about processing under this Controller Policy) in accordance with the Complaint Handling Procedure (see **Appendix 7**).

8. Cooperation with competent supervisory authorities: ***We must always cooperate with competent supervisory authorities.***	We must cooperate with competent supervisory authorities in accordance with the Cooperation Procedure (see **Appendix 8**).
9. Updates to this Controller Policy: ***We will update this Controller Policy in accordance with our Updating Procedure.***	We must update our Controller Policy in accordance with the Updating Procedure (see **Appendix 9**).
10. Conflicts between this Controller Policy and national legislation: ***We must take care where local laws conflict with this Policy, and act responsibly to ensure a high standard or protection for the personal data in such circumstances.***	If local laws applicable to any group member prevent it from fulfilling its obligations under the Controller Policy or otherwise have a substantial effect on its ability to comply with the Controller Policy, the group members must promptly inform the Data Protection Team unless prohibited by a law enforcement authority. The Data Protection Team will make a responsible decision on the action to take. If the laws applicable to a non-European group member are likely to have a substantial adverse effect on its ability to comply with this Controller Policy, the Data Protection Team shall report this issue to the competent supervisory authority. This includes any legally binding request for disclosure of the personal data by a law enforcement authority or state security body, which will be handled as

	set out in **Rule 11** – Ensuring adequate protection for transfers. **10.1 Transparency when legislation prevents compliance with the Controller Policy** In accordance with **Rule 11** – Ensuring adequate protection for transfers, in circumstances where group members are transferring personal data to a third country, each group member shall continually assess whether it has reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the group member importing the data (including any requirements to disclose personal data or measures authorizing access by a public authority) prevent the group member from fulfilling its obligations under the Controller Policy. If the laws and practices in the third country of destination applicable to the processing of the personal data by the group member importing the data prevent it from fulfilling its obligations under, or otherwise have a substantial, adverse effect on the guarantees provided by, the Controller Policy, the group member shall, unless prohibited by law, promptly inform the group member exporting the data and the DPO and comply with the procedure in **Appendix 10**. The DPO will inform Shopify International Limited and the competent supervisory authority about the request, including information about the data requested, the requesting body, and the legal basis for the disclosure, unless otherwise prohibited by law.

	In the event notification to the competent supervisory authority is prohibited, the DPO and the group member will use its best efforts to obtain the right to waive this prohibition in order to communicate as much information as it can as soon as possible and to be able to demonstrate that it did so. If, despite having used its best efforts, the DPO on behalf of the group member is not in a position to notify the competent supervisory authority, the DPO on behalf of the group member shall annually provide general information on the requests it received to the competent supervisory authority including the number of applications for disclosure, type of data requested, requesting authority or authorities, whether requests have been challenged and the outcome of such challenges. Group members acknowledge that transfers of personal data by a group member to any public authority cannot be massive, disproportionate or indiscriminate in a manner that would go beyond what is necessary in a democratic society. **10.2 Relationship between national laws and the Controller Policy** Group members must process personal data in accordance with the Controller Policy. Where the national legislation requires a higher level of protection for personal data, such national legislation shall take precedence over this Controller Policy. In accordance with **Rule 11**, each group member established outside Europe will ensure that it has no

	reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the group member importing the data (including any requirements to disclose personal data or measures authorizing access by public authorities) prevent the group member from fulfilling its obligations under the Controller Policy. In giving this assurance, each relevant group member has undertaken and documented an assessment in particular considering the following elements: ● the specific circumstances of the transfer, including: o the type of recipients; o economic sector in which the transfer occurs; o the purpose of processing; o the categories and format of the personal data; o the location of the processing, including storage; and o the transmission channels used. ● the laws and practices of the country in which the group member is established in light of the circumstances of the transfer, including those requiring to disclose data to public authorities or

	authorising access by such authorities, as well as the applicable limitations and safeguards; and ● any safeguards in addition to those under the Controller Policy, including the technical and organisational measures applied during transmission and to the processing of the personal data in the country of destination in which the group member is established. Shopify will make available a non-privileged summary of this assessment to a supervisory authority on request. Where a group member importing the data from Europe has reason to believe that it is or has become subject to laws or practices in the country of destination applicable to the processing of the personal data by the group member importing the data, including following a change in the laws of the country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the Controller Policy, the group member importing the data from Europe shall promptly notify the group member exporting the data from Europe and both parties shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the group members to address the situation. The group member exporting the data shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by a competent supervisory authority to do so. The group member

	importing the data will promptly inform the DPO of the issue in accordance with **commitment 10.1** of Part III. The DPO will inform Shopify International Limited and report the issue to the competent supervisory authority unless prohibited by law. In the event notification to the competent supervisory authority is prohibited, the DPO and the group member will follow the process in **commitment 10.1** of Part III. Where a group member receives any legally binding request for disclosure of personal data by a law enforcement authority or becomes aware of any direct access by public authorities to personal data transferred pursuant to the Controller Policy it shall comply with the procedure in **Appendix 10**.
11. Government requests for disclosure of personal data: ***We must comply with our Government Disclosure Request Procedure in case of a legally binding request for disclosure of personal data.***	If a group member receives a legally binding request for disclosure of personal data from a law enforcement authority or state security body which is subject to this Controller Policy, it must comply with the Government Disclosure Request Procedure set out in **Appendix 10**.
12. Termination	In the event that a group member acting as data importer ceases to be bound by this Controller Policy, the group member may keep the data provided to it by the data exporter provided that arrangements have been put in place between the group member acting as data importer and the group member acting as data exporter to ensure

	that the continued processing of the data by the data importer complies with the requirements regarding transfers contained in European data protection law, otherwise the data must be returned to the group member acting as data exporter.
13. Non-Compliance	Shopify will ensure that no transfer is made to a group member unless the group member is effectively bound by the Controller Policy and can deliver compliance. A group member importing personal data from Europe will promptly inform the Data Protection Team if it is unable to comply with the Controller Policy, for whatever reason, including the situations further described under **commitment 10** of Part III of this Controller Policy. The Data Protection Team will then notify the relevant data exporter. Where the group member importing the personal data is in breach of the Controller Policy or unable to comply with them, the group member exporting the personal data will suspend the transfer. The group member importing the personal data will, at the choice of the group member exporting the personal data, immediately return or delete the personal data (and any copies of the personal data) that has been transferred under the Controller Policy in its entirety, where: ● the group member exporting the personal data has suspended the transfer, and compliance with this

	Controller Policy is not restored within a reasonable time, and in any event within one month of suspension; or ● the group member importing the personal data is in substantial or persistent breach of the Controller Policy; or ● the group member importing the personal data fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under the Controller Policy. The group member importing the personal data will certify the deletion of the data to the group member exporting the personal data. Until the data is deleted or returned, the group member importing the personal data will ensure compliance with the Controller Policy. In the event that local laws applicable to the group member importing the personal data prohibit the return or deletion of the transferred personal data, the group member importing the personal data will ensure that it will continue to ensure compliance with the Controller Policy, and will only process the personal data to the extent and for as long as required under that local law.

Part IV: Third Party Beneficiary Rights

Application of this Part IV

This Part IV applies where data subjects' personal data are protected under European Data Protection Laws (including the General Data Protection Regulation). This is the case when:

- those data subjects' personal data are processed in the context of the activities of a group member (or its third party processor) established in Europe;
- a non-European group member (or its third-party processor) offers goods and services (including free goods and services) to those data subjects in Europe; or
- a non-European group member (or its third-party processor) monitors the behaviour of those data subjects, as far as their behaviour takes place in Europe;

and that group member then transfers those data subjects' personal data to a non-European group member for processing under the Controller Policy.

Entitlement to effective remedies

When this Part IV applies, data subjects have the right to pursue effective remedies in the event their personal data is processed by Shopify in breach of the following provisions of this Controller Policy:

- Part II (Our Obligations) of this Controller Policy;
- Paragraphs 7 (Complaint Handling), 8 (Cooperation with Competent Supervisory Authorities), 9 (Updates to this Controller Policy), 10 (Conflicts between this Controller Policy and national legislation) and 11 (Government requests for disclosure of personal data) under Part III of this Controller Policy; and
- Part IV (Third Party Beneficiary Rights) of this Controller Policy.

For the avoidance of doubt, these rights do not extend to those elements of the Controller Policy pertaining to internal mechanisms implemented within entities, such as details of training, audit programme, compliance network, and mechanism for updating the Controller Policy.

Data subjects' third party beneficiary rights

When this Part IV applies, data subjects may exercise the following rights:

- Complaints: Data subjects may complain to a group member and/or to a European supervisory authority, in accordance with the Complaint Handling Procedure at **Appendix 7**;

- Proceedings: Data subjects may commence proceedings against a group member for violations of this Controller Policy, in accordance with the Complaint Handling Procedure at **Appendix 7**;

- Compensation: Data subjects who have suffered damage as a result of an infringement of this Controller Policy have the right to receive compensation from Shopify for the damage suffered; and

- Transparency: Data subjects also have the right to obtain a copy of the Controller Policy upon request to Shopify's Data Protection Team. A copy of the Controller Policy will also be made available online on Shopify's website at **www.shopify.com/legal**.

The group members accept that data subjects may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) GDPR.

Responsibility for breaches by non-European group members

Shopify International Limited will be responsible for ensuring that any action necessary is taken to remedy any breach of this Controller Policy by a non-European group member.

In particular:

- If a data subject can demonstrate damage it has suffered likely occurred because of a breach of this Policy by a non-European group member, Shopify International Limited will have the burden of proof to show that the non-European group member is not responsible for the breach, or that no such breach took place;

- where a non-European group member fails to comply with this Controller Policy, data subjects may exercise their rights and remedies above against Shopify International Limited and, where appropriate, receive compensation (as determined by a competent court or other competent authority) from Shopify International Limited for any material or non-material damage suffered as a result of a breach of this Controller Policy.

Shared liability for breaches with processors

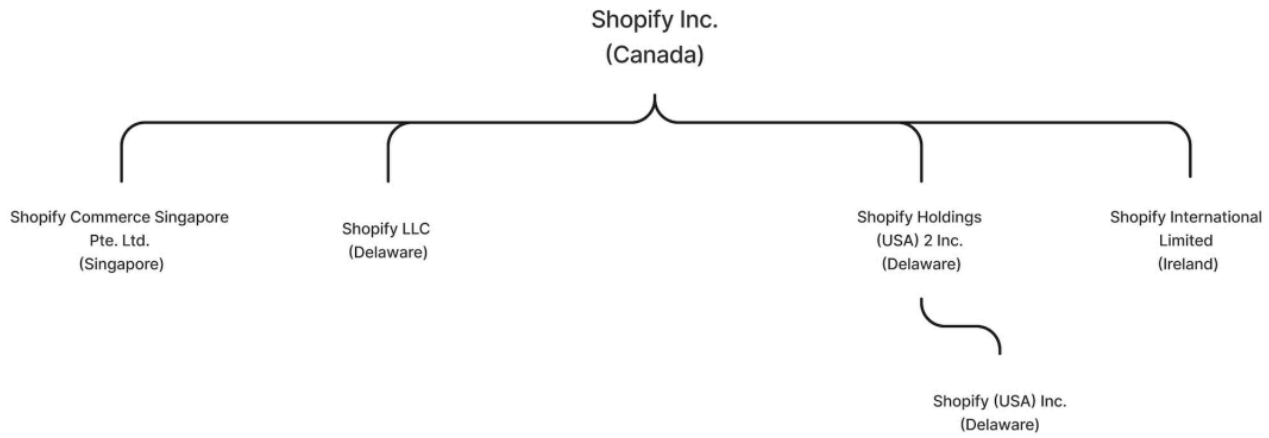
Where Shopify has engaged a third-party processor to conduct processing on its behalf, and both are responsible for harm caused to an individual by processing in breach of this Controller Policy, Shopify accepts that both Shopify and the processor may be held liable for the entire damage in order to ensure effective compensation of the data subject.

Part V: Appendices

Appendix 1 – Shopify Group Members

SHOPIFY GROUP MEMBERS

The following chart shows our current material subsidiaries. These subsidiaries are, directly or indirectly, wholly owned by Shopify Inc., which is a Canadian registered publicly traded company.



The tables below list the Shopify group members which are bound by Shopify's "Binding Corporate Rules: Controller Policy".

Entities Located Within Europe		
Entity	**Contact details and registration number**	**Country**
Shopify International Limited	Address: 2nd Fl. Victoria Buildings 1-2 Haddington Rd.; Dublin 4, D04 XN32; Ireland privacyoffice@shopify.com Reg no.: 560279	Ireland
Shopify Lithuania UAB	Address: Žalgirio st. 90-100, corpus D, 6th floor, 09303; Vilnius; Lithuania	Lithuania

	privacyoffice@shopify.com Reg no.: 303888502	
Shopify Commerce Germany GmbH	Address: Köpenicker Str. 90, 10179 Berlin, Germany privacyoffice@shopify.com Reg no.: HRB 182879B	Germany
Shopify Sweden AB	Address: Box 16285, 103 25, Stockholm, Sweden privacyoffice@shopify.com Reg no.: 556838-0082	Sweden
Shopify Commerce France, SAS	Address: 74 Rue de Rome, 75008 Paris, France privacyoffice@shopify.com Reg. no.: 902 633 577	France
Shopify Commerce Spain, S.L.	Address: Carrer de Roc Boronat 147, 10º 08018, Barcelona, Spain privacyoffice@shopify.com Reg. no.: B-67.618.447	Spain
Shopify Commerce Netherlands B.V.	Address: Basisweg 10, 1043 AP, Amsterdam, The Netherlands privacyoffice@shopify.com Reg. no.: CCI 82284059	The Netherlands
Shopify Commerce Poland sp. z.o.o.	Address: ul. Jasna 26, 00-054 Warszawa, Poland privacyoffice@shopify.com Reg. no.: 0000926665	Poland
Shopify Commerce Italy S.r.l.	Address: Piazza San Babila, 1, 20122, Milan, Italy privacyoffice@shopify.com Reg. no: MI – 2662935	Italy
Suprb AB	Address: Box 16285, 103 25 Stockholm, Sweden	Sweden

Entities Located Outside of Europe		
Entity	**Contact details and registration number**	**Country**
Shopify Inc.	Address: 151 O'Connor Street, Ground floor, Ottawa, ON K2P 2L8. Canada	Canada

	privacyoffice@shopify.com Reg no.: 426160-7	
Shopify Payments (Canada) Inc.	Address: 151 O'Connor Street, Ground floor, Ottawa, ON K2P 2L8, Canada privacyoffice@shopify.com Reg no.: 716589-7	Canada
Shopify Studios Holdings Inc.	Address: 151 O'Connor Street, Ground floor, Ottawa, ON K2P 2L8, Canada privacyoffice@shopify.com Reg no.: 1112588-5	Canada
Future of Work Film Inc.	Address: 151 O'Connor Street, Ground floor, Ottawa, ON K2P 2L8, Canada privacyoffice@shopify.com Reg no.: 1113027-7	Canada
Shopify Quebec Inc.	Address: 151 O'Connor Street, Ground floor, Ottawa, ON K2P 2L8, Canada privacyoffice@shopify.com Reg no.: 1348064-0	Canada
Shopify Payment Activities Inc.	Address: 151 O'Connor Street, Ground Floor, Ottawa, Ontario, K2P 2L8, Canada privacyoffice@shopify.com Reg no.: 1001056939	Canada
Shopify LLC	Address: 251 Little Falls Drive, Wilmington, DE 19808, USA privacyoffice@shopify.com Reg no.: 5504138	USA
Shopify Holdings (USA) 2 Inc.	Address: 251 Little Falls Drive, Wilmington, DE 19808, USA privacyoffice@shopify.com Reg no.: 7518523	USA
Shopify Capital Inc.	Address: 100 Shockoe Slip, 2nd Floor Richmond, VA 23219, USA privacyoffice@shopify.com Reg no.: 0800365-9	USA

Shopify Payments (USA) Inc.	Address: 251 Little Falls Drive, Wilmington, DE 19808, USA privacyoffice@shopify.com Reg no.: 4908573	USA
Shopify (USA) Inc.	Address: 251 Little Falls Drive, Wilmington, DE 19808, USA privacyoffice@shopify.com Reg no.: 5515561	USA
DONDE FASHION, INC.	Address: 251 Little Falls Drive, Wilmington, DE 19808, USA privacyoffice@shopify.com Reg. no.: 5501757	USA
SHOPIFY GLOBAL INC.	Address: 251 Little Falls Drive, Wilmington, DE 19808, USA privacyoffice@shopify.com Reg. no.: 6433258	USA
Shopify Strategic Holdings 3 LLC	Address: 251 Little Falls Drive, Wilmington, DE 19808, USA privacyoffice@shopify.com Reg. no.: 6693875	USA
Remix Software Inc.	Address: 251 Little Falls Drive, Wilmington, DE 19808, USA privacyoffice@shopify.com Reg. no.: 5931027	USA
Shopify Strategic Holdings 4 LLC	Address: 251 Little Falls Drive, Wilmington, DE 19808, USA privacyoffice@shopify.com Reg. no.: 7141222	USA
Shopify Strategic Holdings 5 LLC	Address: 251 Little Falls Drive, Wilmington, DE 19808, USA privacyoffice@shopify.com Reg. no.: 7426352	USA

Shopify Rebellion LoL Inc.	Address: 251 Little Falls Drive, Wilmington, DE 19808, USA privacyoffice@shopify.com Reg. no.: 7626618	USA
Checkout Blocks Inc.	Address: 251 Little Falls Drive, Wilmington, DE 19808, USA privacyoffice@shopify.com Reg. no.: 7041938	USA
ChannelApe, Inc.	Address: 251 Little Falls Drive, Wilmington, DE 19808, USA privacyoffice@shopify.com Reg. no.: 6278610	USA
SC Commerce Services Inc.	Address: 251 Little Falls Drive, Wilmington, DE 19808, USA privacyoffice@shopify.com Corp. no.: 4756665	USA
Shopify Financial Services Inc.	Address: 251 Little Falls Drive, Wilmington, DE 19808, USA privacyoffice@shopify.com Corp. no.: 10042839	USA
Shopify Rebellion Inc.	Address: Address: 251 Little Falls Drive, Wilmington, DE 19808, USA privacyoffice@shopify.com Corp. no.: 10066611	USA
Shopify Rebellion Brand Inc.	Address: Address: 251 Little Falls Drive, Wilmington, DE 19808, USA privacyoffice@shopify.com Corp. no.: 10066614	USA
Shopify Search, Inc.	Address: Address: 251 Little Falls Drive, Wilmington, DE 19808, USA privacyoffice@shopify.com Corp. no.: 7463024	USA

Shopify (Australia) Pty. Ltd.	Address: c/- Intertrust Australia, Level 25, Suite 2, 100 Miller Street, North Sydney 2060 NSW, Australia privacyoffice@shopify.com Reg no.: 608 159 860	Australia
Shopify Commerce India Private Limited	Address: No. 10, Ground Floor, Park Road, Tasker Park, Tasker Town, Shivaji Nagar, Near Indian Express, H.K.P. Road, Bangalore North, Bangalore KA – 560051, India privacyoffice@shopify.com Reg no.: U74999KA2017FTC102908	India
Shopify Japan Kabushiki Kaisha	Address: 6-12-18 Jingumae, Shibuya-ku, Tokyo, 150-0001, Japan privacyoffice@shopify.com Reg no.: 10001187930	Japan
Shopify Commerce Singapore PTE. LTD.	Address: 77 Robinson Rd., #13-00 Robinson 77, Singapore 068896 privacyoffice@shopify.com Reg no.: 201736986Z	Singapore
Shopify UK Limited	Address: 1 Bartholomew Lane, London, EC2N 2AX, UK privacyoffice@shopify.com Reg no.: 11256480	UK
Shopify Commerce New Zealand Limited	Address: C/o Bell Gully, Level 4, 40 Lady Elizabeth Lane, Wellington Central, Wellington, 6011, New Zealand privacyoffice@shopify.com Reg no.: 9429046669346	New Zealand
Donde Mobile R&D Ltd.	Address: 20 HaHarash St., Tel Aviv-Yafo 6761310, Israel	Israel

	privacyoffice@shopify.com Reg. no: 515098952	
Concrete Utopia Limited	Address: 1 Bartholomew Lane, London, United Kingdom, EC2N 2AX privacyoffice@shopify.com Reg. no: 09519543	UK
Shopify Commerce Brazil Ltda	Address: Avenida Paulista, 37 - Conj 41, Bela Vista, São Paulo, 01311-902, Brazil privacyoffice@shopify.com Reg. no: 35260280991	Brazil
Shopify TAF (USA) Inc.	Address: Address: 251 Little Falls Drive, Wilmington, DE 19808, USA privacyoffice@shopify.com Corp. no.: 7463024	USA
Shopify Technology (USA) Inc.	Address: 85 10th Ave, Suite 800, New York, NY 10011, USA privacyoffice@shopify.com	USA

Appendix 2 - Fair Information Disclosures

1. Background

1.1 This Fair Information Disclosure document sets out the transparency information that Shopify must provide to data subjects when processing their personal data under Shopify's Controller Policy.

2. Information to be provided where Shopify collects personal data directly from data subjects

2.1 When Shopify collects personal data directly from data subjects, it must provide the following transparency information:

(a) the **identity and contact details** of the data controller and, where applicable, of its representative;

(b) the contact details of the **data protection officer**, where applicable;

(c) the **purposes** of the processing for which the personal data are intended as well as the **legal basis** for the processing;

(d) where the processing is based on Shopify's or a third party's legitimate interests, the **legitimate interests** pursued by Shopify or by the third party;

(e) the **recipients or categories of recipients** of the personal data, if any;

(f) where applicable, the fact that a group member in Europe intends to **transfer** personal data to a third country or international organisation outside of Europe, and the measures that the group member will take to ensure the personal data remains protected in accordance with applicable data protection laws and how to obtain a copy of such measures.

2.2 In addition to the information above, Shopify shall also provide data subjects with the following further information necessary to ensure fair and transparent processing, at the time of collection:

(a) the **period** for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

(b) information about the **data subjects' rights** to request access to, rectify or erase their personal data, as well as the right to restrict or object to the processing, and the right to data portability;

(c) where the processing is based on consent, the existence of the right to **withdraw consent** at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

(d) the right to **lodge a complaint** with the competent supervisory authority;

(e) whether the provision of personal data is a **statutory or contractual** requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;

(f) the existence of **automated decision-making**, including profiling, and, where such decisions may have a legal effect or significantly affect the data subjects whose personal data are collected, any meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for those data subjects.

2.3 The transparency information described in this paragraph must be provided at the time that Shopify obtains the personal data from the data subject.

3. Information to be provided where Shopify collects personal data about data subjects from a third party source

3.1 When Shopify collects personal data from a third party source (that is, someone other than the data subject him- or herself), it must provide the following transparency information:

(a) the information described in paragraphs 2.1 and 2.2 above;

(b) the categories of **personal data** that are being processed; and

(c) **details of the third party source** from which Shopify obtained the personal data including, if applicable, identifying whether the personal data came from publicly accessible sources.

3.2 The transparency information described in this paragraph must be provided within a reasonable period after Shopify obtains the personal data and, at the latest, within one month, having regard to the specific circumstances in which the personal data are processed. In addition:

(a) if the personal data are to be used for communication with the data subject, the transparency information described in this paragraph must be provided at the latest at the time of the first communication to that data subject; and

(b) if a disclosure of the personal data to another recipient is envisaged, the transparency information described in this paragraph must be provided at the latest when the personal data are first disclosed.

4. Derogations from providing transparency disclosures

4.1 The requirements to provide transparency information as described in this Fair Information Disclosures document shall not apply where and insofar as:

(a) the data subject already has the information;

(b) the provision of such information provides impossible or would involve a disproportionate effort, and Shopify takes appropriate measures, consistent with the requirements of applicable data protection laws, to protect the data

subject's rights and freedoms and legitimate interests, including by making the transparency information publicly available;

(c) obtaining or disclosure is expressly laid down by applicable laws to which Shopify is subject and these laws provide appropriate measures to protect the data subject's legitimate interests;

(d) where the personal data must remain confidential subject to an obligation of professional secrecy regulated by applicable laws to which Shopify is subject, including a statutory obligation of secrecy.

Appendix 3 - Data Protection Rights Procedure

1. Introduction

1.1 Data subjects whose personal data are processed by Shopify under Shopify's Controller Policy have certain data protection rights, which they may exercise by making a request to the controller of their information (a "**Data Request**").

1.2 This Binding Corporate Rules: Data Protection Rights Procedure ("**Data Protection Rights Procedure**") describes how Shopify will respond to any Data Requests it receives from data subjects whose personal data are processed and transferred under the Controller Policy.

2. Data subject's data protection rights

2.1 Shopify must help data subjects exercise the following data protection rights, consistent with the requirements of applicable data protection laws:

(a) **The right of access:** This is the right for data subjects to obtain confirmation whether a controller processes personal data about them and, if so, to be provided with details of that personal data and access to it. This process for handling this type of request is described further in paragraph 4 below.

(b) **The right to rectification:** This is the right for data subjects to obtain from a controller without undue delay the rectification of any inaccurate personal data a controller may be processing about them. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement. The process for handling this type of request is described further in paragraph 5 below.

(c) **The right to erasure:** This is the right for data subjects to obtain from a controller the erasure of personal data without undue delay where one of the

following grounds apply: (i) the personal data are no longer necessary in relation to the purposes for which they were collected or processed, (ii) the data subject has withdrawn their consent to the processing and there is no other legal ground for processing, (iii) the data subject objects to the processing and there are no overriding legitimate grounds for processing or the data subject objects to the processing of personal data for direct-marketing purposes, (iv) the personal data have been unlawfully processed, (v) the personal data have to be erased for compliance with a legal obligation to which the controller is subject, or (vi) the personal data have been collected in relation to the offer of information society services to children. Where the controller has made the personal data public and is obliged on request to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, unless this proves impossible or involves disproportionate effort, to inform recipients processing the personal data that the data subject has requested the erasure of any links to or copy or replication of those personal data. The controller shall inform the data subject about those recipients if the data subject requests about them on certain grounds – for example, where the personal data is no longer necessary to fulfil the purposes for which it was collected. This right does not apply to the extent the processing is necessary for: (i) exercising the right to freedom of expression and information, (ii) for compliance with an obligation to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, (iii) for reasons of public interest in the area of public health, (iv) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, or (v) for the establishment, exercise or defence of legal claims. The process for handling this type of request is described further in paragraph 5 below.

(d) **The right to restriction:** This is the right for data subjects to obtain from a controller restriction of processing of personal data about them where one of

the following applies: (i) the accuracy of the personal data is contested by the data subject, in which case processing shall be restricted for a period enabling the controller to verify the accuracy of the personal data, (ii) the processing is unlawful and the individual opposes the erasure of the personal data and requests the restriction of their use instead, (iii) the controller no longer needs the personal data for the purposes of the processing for which they were kept, but the data subject requests they be kept for the establishment, exercise, or defence of legal claims, or (iv) the data subject has objected to processing pursuant to (e) below pending verification of whether the legitimate grounds of the controller override those of the data subject. Where processing has been restricted, the personal data shall, with the exception of storage, only be processed with the data subject's consent, for the establishment, exercise, or defence of legal claims or for the protection of the rights of another natural or legal person, or for reasons of important public interest set out in the law of origin of the personal data. A data subject shall be informed by the controller before the restriction of processing is lifted. The controller shall communicate any restriction of processing request to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the individual about those recipients if the individual requests on certain grounds. The process for handling this type of request is described further in paragraph 5 below.

(e) **The right to object:** This is the right for data subjects to object, on certain grounds relating to their particular situation, to a controller's processing of personal data about them where such processing is based on the performance of a task carried out in the public interest or the controller's or a third party's legitimate interest. The controller shall no longer process the personal data unless (i) the controller demonstrates that compelling, legitimate grounds for the processing override the interests of the data subject or (ii) for the establishment, exercise, or defence of a legal claim. At any time, a data subject may object to the processing of personal data for direct marketing purposes,

which include profiling to the extent that it relates to the direct marketing. Where the data subject objects to processing for direct-marketing purposes, the personal data shall no longer be processed for such purposes. Where personal data are processed for scientific or historical research purposes or statistical purposes, the data subject, on grounds relating to their particular situation, shall have the right to object to processing of personal data concerning them, unless the processing is necessary for the performance of a task carried out for reasons of public interest. The process for handling this type of request is described further in paragraph 5 below.

(f) **The right to data portability:** This is the right for data subjects to receive personal data concerning them from a controller in a structured, commonly used and machine-readable format and to transmit that data to another controller where: (i) the processing is based on consent or necessity for the performance of a contract, and (ii) the processing is carried out by automated means, if certain grounds apply. The process for handling this type of request is described further in paragraph 6 below.

3. Responding to a Data Request

3.1 *Overview*

3.1.1 The controller of a data subject's personal data is primarily responsible for responding to a Data Request and for helping the data subject concerned to exercise his or her rights under applicable data protection laws.

3.1.2 As such, when a data subject contacts Shopify to make any Data Request under the Controller Policy, it must help the data subject to exercise his or her data protection rights directly in accordance with this Data Protection Rights Procedure. In doing so, Shopify will employ automated tools and processes, where appropriate, to ensure it complies with its obligations.

3.2 *Assessing the obligation to respond to a Data Request*

3.2.1 If a group member receives a Data Request from a data subject, such a request will be passed to the Data Protection Team and other designated teams immediately upon receipt and in any event not later than 7 days after having become aware of the request, indicating the date on which it was received together with any other information which may be relevant to help deal with the request.

3.2.2 An initial assessment of the Data Request will be made as follows:

(a) it will be determined whether Shopify is a controller or processor of the personal data that is the subject of the Data Request; and

(b) where it is determined that Shopify is a controller of the personal data, it will then be determined whether the Data Request is valid under applicable data protection laws (in accordance with paragraph 3.3 below) and/or whether an exemption applies (in accordance with paragraph 3.4 below), and a response will be provided to the Request (in accordance with paragraph 3.5 below).

3.3 Assessing the validity of a Data Request

3.3.1 If the Data Protection Team and other designated teams determine that Shopify is the controller of the personal data that is the subject of the Data Request, they will first assess the validity of the request under applicable data protection laws.

3.3.2 A Data Request must generally be made in writing, which can include email or online interfaces provided by Shopify. A Data Request does not have to be official or mention data protection law to qualify as a valid request.

3.3.3 If Shopify has reasonable doubts concerning the identity of the data subject making a request, it may request such additional information as is necessary to confirm the identity of the data subject making the request. Shopify may also request any further information which is necessary to action the data subject's request.

3.4 Exemptions to a Data Request

3.4.1 Shopify will not refuse to act on a valid Data Request unless it can demonstrate that an exemption applies under applicable data protection laws.

3.4.2 Shopify may be exempt under applicable data protection laws from fulfilling the Data Request if it can demonstrate that the data subject has made a manifestly unfounded or excessive Data Request (in particular, because of the repetitive character of the request).

3.4.3 If Shopify decides not to take action on the Data Request, Shopify will inform the data subject without delay and at the latest within one (1) month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with the competent supervisory authority (as described in **Appendix 7** - Complaint Handling Procedure) and seeking a judicial remedy.

3.5 *Responding to a Data Request*

3.5.1 Where Shopify is the controller of the personal data that is the subject of the Data Request, and Shopify has already confirmed the identity of the requestor and has sufficient information to enable it to fulfil the request (and no exemption applies under applicable data protection laws), then Shopify shall deal with the Data Request in accordance with paragraphs 4, 5 and/or 6 below (as appropriate).

3.5.2 Shopify will respond to a Data Request without undue delay and in no case later than one (1) month of receipt of that request. This one (1) month period may be extended by two (2) further months where necessary, for example if the request is complex or due to the number of requests that have been made. Shopify will inform the data subject of any such extension within one (1) month of receipt of the Data Request, together with the reasons for the delay. Records about the requests will be kept by Shopify for a minimum of two (2) years.

4. **Requests for Access to Personal Data**

4.1 *Overview*

4.1.1 A data subject may, under applicable data protection laws, require a controller to provide the following information concerning processing of his or her personal data:

(a) confirmation as to whether the controller holds and is processing personal data about that data subject;

(b) if so, a description of the purposes of the processing, the categories of personal data concerned, the recipients or categories of recipients to whom the information is, or may be, disclosed, the envisaged period(s) (or the criteria used for determining those period(s)) for which the personal data will be stored;

(c) information about the data subject's right to request rectification or erasure of his or her personal data, or to restrict or object to its processing;

(d) information about the data subject's right to lodge a complaint with a competent supervisory authority;

(e) information about the source of the personal data if it was not collected directly from the data subject;

(f) details about whether the personal data is subject to automated decision-making (including automated decision-making based on profiling); and

(g) where personal data is transferred outside Europe, the appropriate safeguards that Shopify has put in place relating to such transfers in accordance with applicable data protection laws.

4.1.2 A data subject may also be entitled to request a copy of his or her personal data from the controller. Where a data subject makes a valid request of this type, the controller must provide that personal data to the data subject in intelligible form.

4.2 *Process for responding to access requests from data subjects*

4.2.1 If Shopify receives an access request from a data subject, such a request will be passed to the Data Protection Team and other designated teams, and a prompt initial assessment of responsibility will be made consistent with the requirements of paragraph 3.2 above.

4.2.2 Where Shopify determines it is the controller of the personal data and responsible for responding to the data subject directly (and that the request is valid and that no exemption to the right of access applies under applicable data protection laws), the Data Protection Team and other designated teams will work to arrange a search of all relevant data sources.

4.2.3 The Data Protection Team and other designated teams may refer any complex cases to the senior management for advice, including where the request concerns information relating to third parties or where the release of personal data may include trade secrets.

4.2.4 The personal data that must be disclosed to the data subject will be compiled in a readily understandable format. A cover letter (or cover email) will be prepared, which includes all information required to be provided in response to a data subject's access request (including the information described in paragraph 4.1.1).

4.3 *Exemptions to the right of access*

4.3.1 An otherwise-valid Data Request may be refused on grounds such as:

(a) If the refusal to provide the information is consistent with applicable data protection law (for example, where a European group member transfers personal data under the Controller Policy, if the refusal to provide the information is consistent with the applicable data protection law in the European country where the group member is located);

(b) where the personal data is processed by Shopify by non-automated means and the personal data does not and will not form part of a filing system, within the meaning of the GDPR; or

(c) where providing a copy of the personal data concerned would adversely affect the rights of others, which may include other data subjects' personal data or trade secrets.

4.3.2 The Data Protection Team and other designated teams will assess each Data Request individually to determine whether any applicable exemptions apply. A group member must never apply an exemption unless this has been discussed and agreed with the Data Protection Team and other designated teams.

5. Requests to correct, update or erase personal data, or to restrict or cease processing personal data

5.1 If Shopify receives a request to correct, update or erase personal data, or to restrict or cease processing of a data subject's personal data, such a request will be passed to the Data Protection Team and other designated teams immediately, and an initial assessment will be made of responsibility consistent with the requirements of paragraph 3.2 above.

5.2 Where such initial assessment of responsibility reveals that Shopify is the controller of that personal data, the request must be communicated to the Data Protection Team and other designated teams for it to consider and deal with as appropriate in accordance with applicable data protection laws.

5.3 When Shopify must rectify, restrict or erase personal data, in its capacity as controller, Shopify will notify other group members and any processor to whom the personal data has been disclosed so that they can also update their records accordingly.

5.4 If Shopify acting as controller has made the personal data public, and is obliged to erase the personal data pursuant to a Data Request, it must take reasonable steps, including technical measures where feasible (taking account of available technology and the cost of implementation), to inform other controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, the personal data.

6. **Requests for data portability**

6.1 If a data subject makes a Data Request to Shopify acting as controller to receive the personal data that they have provided to Shopify in a structured, commonly used and machine-readable format and/or to transmit directly such information to another controller (where technically feasible), Shopify's Data Protection Team and other designated teams will consider and deal with the request appropriately in accordance with applicable data protection laws (including taking into account that the right to data portability must not adversely affect the rights of others, which may include other data subjects' personal data or trade secrets) insofar as the processing is based on that data subject's consent or on the performance of, or steps taken at the request of the data subject prior to entry into, a contract.

7. **Questions about this Data Protection Rights Procedure**

7.1 All questions relating to this Data Protection Rights Procedure are to be addressed to the Data Protection Team at privacyoffice@shopify.com.

Appendix 4 - Privacy Compliance Structure

1. Introduction

1.1 Shopify’s compliance with global data protection laws and the Controller Policy is overseen and managed throughout all levels of the business by a global, multi-layered, cross-functional privacy compliance structure. Further information about Shopify's Data Protection Team, Privacy Working Group and Regulatory Affairs and Enforcement Team is set out below.

2. The Data Protection Team

2.1 Shopify's Data Protection Team is composed of members of the Legal Team, the DPO and their supporting staff members. The Data Protection Team is responsible for managing and implementing Shopify's data protection program internally (including the Policies) and is actively engaged in addressing matters relating to Shopify's privacy compliance on a routine, day-to-day basis.

2.2 The DPO reports directly to the Shopify International Board. The DPO will not conduct any tasks that could result in a conflict of interest. For example, the DPO will not be in charge of conducting data protection impact assessments or carrying out audits of the Controller Policy.

2.3 The Data Protection Team's key responsibilities include:

(a) implementing and overseeing privacy and data protection compliance practices within Shopify that are consistent with the requirements of applicable data protection laws, Shopify’s policies, strategies and business objectives;

(b) periodically assessing Shopify’s privacy and data protection compliance measures, accomplishments, and resources to ensure their continued effectiveness and identify and action improvements where necessary;

(c) ensuring that effective privacy and data protection controls exist whenever Shopify independently (i.e. not at the instruction of a third party Controller) discloses personal data to a third party service provider;

(d) responding to inquiries and complaints relating to the Policies from staff members, merchants and other third parties raised through Shopify's Customer Support portal; and overseeing compliance with the Binding Corporate Rules: Complaint Handling Procedure and the Binding Corporate Rules: Data Protection Rights Procedure and the handling of any complaints or requests made under them;

(e) discussing with senior management the privacy and data protection legal and regulatory requirements applicable to Shopify and its compliance with such requirements, and where appropriate, making recommendations to the Board with respect to Shopify's privacy and data protection policies and procedures to ensure ongoing compliance with applicable data protection laws and regulations;

(f) periodically reviewing and assessing the continued effectiveness and adequacy of its responsibilities as outlined in this document; and where necessary, notifying the Board of any amendments or modifications it believes are necessary;

(g) instituting and ensuring the adequacy of Shopify's data protection training program for staff and independent contractors that have access to personal data in accordance with the Binding Corporate Rules: Privacy Training Program;

(h) promoting privacy awareness across all business units and Shopify locations through data protection communications and awareness-raising initiatives;

(i) ensuring that any material updates to its privacy and data protection policies are communicated to staff and, where required, merchants, Shopify customers and/or regulatory authorities and supervisory authorities;

(j) overseeing audits of the Policies, ensuring audits address all aspects of the Policies, coordinating responses to audit findings and responding to inquiries of the supervisory authorities;

(k) where requested, advising the business teams as regard to data protection impact assessments and monitor its performance;

(l) regularly assessing whether Shopify's privacy and data protection policies, procedures and guidance expose Shopify to any material compliance risks and, where this is the case, identifying the steps that Shopify may take to mitigate or remedy such risks; elevating material concerns or questions to the Board, if the matter may have a material effect on Shopify's finances, reputation, or its privacy and data protection policies and procedures; and

(m) cooperating with, and being a contact point for, supervisory authorities.

3. **Privacy Working Group**

3.1 Shopify has established a privacy and data protection working group (the **"Privacy Working Group"**) whose role is to oversee the technical and product implementations of the privacy requirements and guidance set out by the Data Protection Team.

3.2 *Membership of the Privacy Working Group:* The Privacy Working Group shall consist of a cross-functional group of Shopify employees principally from the Data Protection Team or a similar team (who are responsible for security throughout the company).

3.3 *New members:* Additional or replacement members of the Privacy Working Group shall be nominated and approved by majority approval of the Privacy Working Group. The Chair of the Privacy Working Group shall have the deciding vote in the event of a tied vote.

3.4 The Privacy Working Group's key responsibilities include:

(a) tracking ongoing technical and product work within Shopify to ensure privacy requirements are discussed and any solutions are implemented in accordance with the principles of data protection by design and by default;

(b) discussing potential new products, services, data flows, or systems within Shopify that have privacy implications and to ensure that any technical or engineering solutions are discussed and embedded from an early stage; and

(c) escalating any questions and compliance issues or communicating any actual or potential privacy risks arising from its products, services, data flows, or systems to the Data Protection Team as appropriate.

3.5 *Frequency of Meetings:* The Privacy Working Group shall meet at least once per quarter, and more often if the Privacy Working Group deems it necessary to carry out its responsibilities above, to address a change in the applicable legal or regulatory requirements, or to respond to a data protection or information security incident.

3.6 *Quorum and Voting Requirements:* A majority of the members of the Privacy Working Group shall constitute a quorum for purposes of holding a meeting and the Chair of the Privacy Working Group shall have the deciding vote in the event of a tied vote.

4. Regulatory Affairs and Enforcement Team

4.1 Shopify's Regulatory Affairs and Enforcement Team (the "**Regulatory Affairs and Enforcement Team**") is responsible for reviewing, managing and challenging a request received from a law enforcement or state security body to disclose personal data processed by Shopify in accordance with the procedure set out in **Appendix 10** to the Controller Policy.

Appendix 5 - Privacy Training Requirements

1. Background

1.1 This document sets out the requirements for Shopify to train its staff members on the requirements of the Controller Policy.

1.2 Shopify must train staff members (including new hires, temporary staff and individual contractors whose roles bring them into contact with personal data) on the basic principles of data protection, confidentiality and information security awareness. This must include training on applicable data protection laws, including European data protection laws.

1.3 Staff members who have permanent or regular access to personal data and who are involved in the processing of personal data or in the development of tools to process personal data must receive additional, tailored training on the Controller Policy and specific data protection issues relevant to their role. This training is further described below and will be repeated periodically.

2. Responsibility for the Privacy Training Program

2.1 Shopify's Data Protection Team has overall responsibility for privacy training at Shopify, with input with colleagues from key functional areas, as appropriate. The Data Protection Team will review training from time to time to ensure it addresses all relevant aspects of the Controller Policy.

2.2 Shopify's senior management is committed to the delivery of data protection training courses, and will ensure that staff are required to participate, and given appropriate time to attend such courses. Course attendance must be recorded and monitored via regular audits of the training process.

3. Delivery of the training courses

3.1 Shopify will deliver interactive online training modules, supplemented by tailored training for relevant staff members if appropriate. The courses are designed to be both informative and user-friendly, generating interest in the topics covered. Staff members must correctly answer a set percentage of a series of multiple choice questions for the course to be deemed complete (the percentage to be determined by the Data Protection Team).

3.2 All Shopify staff members must complete data protection training (including training on the Controller Policy):

(a) as part of their onboarding program;

(b) as part of a regular refresher training at least once every two years;

(c) as and when necessary to stay aware of changes in the law; and

(d) as and when necessary to address any compliance issues arising from time to time.

4. **Training on data protection**

4.1 Shopify's training on data protection and the Controller Policy will cover the following main areas:

(a) What is data protection law?

(b) What are key data protection terminology, concepts and principles?

(c) What should Shopify employees do to protect personal data?

(d) An explanation of the Controller Policy

(e) Practical examples of how and when the Controller Policy applies

(f) The rights that the Controller Policy gives to individuals

4.1.2 Where relevant to a staff member's role, training will cover the following procedures under the Controller Policy:

(a) Data Protection Rights Procedure

(b) Audit Protocol

(c) Complaint Handling Procedure

(d) Government Disclosure Request Procedure

5. Training outcomes

5.1 Shopify's training on data protection will be designed to ensure that staff:

(a) understand the basic principles of data privacy, confidentiality and information security;

(b) have a working knowledge of the Controller Policy;

(c) understand the consequences of non-compliance;

(d) understand who within Shopify to contact with questions, complaints, or concerns; and

(e) receive appropriate and specific training to enable them to process personal data in accordance with the Controller Policy.

Appendix 6 - Audit Protocol

1. **Background**

1.1 Shopify must audit its compliance with the Controller Policy on a regular basis. The purpose of these audits will be to ensure that Shopify processes personal data in full compliance with all aspects of the Controller Policy (including methods and action plans ensuring that corrective actions have been implemented). This document describes how and when Shopify will perform such audits ("**Audit Protocol**").

1.2 Although this Audit Protocol describes the formal process by which Shopify will audit its compliance with the Controller Policy, this is only one way in which Shopify ensures that the provisions of the Controller Policy are observed and corrective actions taken as required. In particular, Shopify's Data Protection Team will provide ongoing guidance about the processing of personal data by group members and about Shopify's compliance with the Controller Policy, and will exercise oversight over group members' data processing activities.

2. **Conduct of an audit**

Overview of audit requirements

2.1 Shopify's Data Protection Team oversees compliance with the Controller Policy day to day, in coordination with the Privacy Working Group. The Data Protection Team is responsible for working with internal and/or independent third-party auditors to audit Shopify's compliance with the Controller Policy. The Data Protection Team shall be independent in the performance of their duties related to such audits.

2.2 For any given audit, the Data Protection Team will designate the relevant auditor, consisting either of internal and/or independent third-party auditors, as set out in paragraph 2.5 below. The DPO will not be involved in any audit which gives rise to a conflict with the performance of their other duties. The designated auditor will be responsible for elevating any issues or instances of non-compliance with the Controller

Policy to the attention of the Data Protection Team. Serious non-compliance issues will be escalated to the board of directors of Shopify International Limited where appropriate.

Frequency of audit

2.3 Audits of compliance with the Controller Policy are conducted:

(a) at least once annually in accordance with this Audit Protocol;

(b) at the request of the DPO and/or the board of directors of Shopify International Limited; and

(c) as determined by the Data Protection Team (for example, in response to a specific incident or other indications of non-compliance with the Controller Policy).

Scope of audit

2.4 The specific activities and controls audited may vary from audit to audit. The Data Protection Team will conduct a risk-based analysis to determine the scope of an audit, taking into account relevant criteria such as:

(a) areas of current regulatory focus;

(b) areas of specific or new risks to Shopify;

(c) areas where the systems and/or processes used to safeguard information have changed materially;

(d) use of innovative new tools, systems or technologies;

(e) areas where there have been previous audit findings or complaints;

(f) the amount of time since the last review of a particular system or process; and

(g) the nature and location of the personal data processed.

The audit will take into account relevant IT systems, databases, and policies related to the processing of personal data under this Controller Policy. The audit will also include the main IT systems for which Shopify engages vendors including, for example, cloud hosting systems, payment and invoice services; and content delivery and security network.

Auditors

2.5 Audits of the Controller Policy (including any related procedures and controls) will be overseen by the Data Protection Team. In addition, where deemed necessary by the Data Protection Team, Shopify may appoint independent, experienced and professional auditors acting under a duty of confidence and in possession of the required professional qualifications as necessary to perform audits of the Controller Policy (including any related procedures and controls).

Reporting

2.6 After each audit, the data protection audit reports must be submitted to the Data Protection Team, the board of directors of Shopify International Limited, and where appropriate, to Shopify's ultimate parent board.

2.7 If non-compliance is identified through an audit, by a supervisory authority or otherwise, the group member shall rectify the identified non-compliance without delay. Such non-compliance shall be notified to the DPO. The DPO will be kept informed of resolution measures, will oversee resolution measures and will direct any suspension and resumption of data transfers to that group member. If non-compliance persists and is not resolved without undue delay, then the DPO shall remove the group member from the Controller Policy and the DPO will notify the lead supervisory authority in the annual update.

2.8 Upon request and subject to applicable law and respect for the confidentiality and trade secrets of the information provided, Shopify will provide copies of the results of data protection audits of the Controller Policy (including any related procedures and controls) to the competent supervisory authorities.

2.9 The Data Protection Team is responsible for liaising with competent supervisory authorities for the purpose of providing the information outlined in paragraph 2.8.

Supervisory authority audits

2.10 The competent supervisory authorities may audit group members for compliance with the Controller Policy (including any related procedures and controls) in accordance with the Binding Corporate Rules: Cooperation Procedure. The competent supervisory authorities can have access to the results of an audit on request.

Appendix 7 - Complaint Handling Procedure

1. Background

1.1 This Complaint Handling Procedure describes how Shopify will address and resolve complaints brought by a data subject whose personal data is processed by Shopify under the Controller Policy.

1.2 This procedure will be made available to data subjects whose personal data is processed by Shopify under the Controller Policy.

2. How data subjects can bring complaints

2.1 Any data subject may raise a data protection-related question, concern or complaint (whether related to the Controller Policy or not) by contacting Shopify's Customer Support portal or by writing to us at the address indicated in the Controller Policy under the heading 'How to raise questions or concerns'.

3. Complaints where Shopify is a Controller

3.1 *Who handles complaints?*

3.1.1 The Data Protection Team will handle all questions, concerns, or complaints in respect of personal data for which Shopify is a data controller, such as when Shopify processes personal data about its employees, or about its merchants or business partners, including questions, concerns or complaints arising under the Controller Policy. The Data Protection Team will work with colleagues from relevant product and service lines to address and resolve such questions, concerns and complaints.

3.2 *What is the response time?*

3.2.1 The Data Protection Team will seek to respond to a question, concern or complaint made by a data subject without undue delay, investigating and making a substantive response within one (1) month of receiving the initial enquiry.

3.2.2 If, due to the complexity of the complaint, a substantive response cannot be given within this period, the Data Protection Team will advise the data subject accordingly and provide a reasonable estimate (not exceeding a further two (2) months) of the time period within which a substantive response will be provided.

3.3 *What happens if a data subject disputes a finding?*

3.3.1 If the data subject notifies the Data Protection Team that it disputes any aspect of the response, the Data Protection Team will refer the matter to the DPO and, in serious cases, to senior management for review. The DPO (and, where appropriate, senior management) will review the case and advise the data subject of its decision either to accept the original finding or to substitute a new finding. The DPO will respond to the complainant within one (1) month from receipt of the data subject's notice of dispute. If the data subject is not satisfied by the decision of the DPO, the DPO will inform the data subject that he/she has the right to lodge a complaint before a supervisory authority).

3.3.2 As part of its review, the DPO may arrange to meet the parties to the dispute, either in person or telephonically, in an attempt to resolve it. If, due to the complexity of the dispute, a substantive response cannot be given within one (1) month of receipt of the data subject's notice of dispute, the DPO will advise the complainant accordingly and provide a reasonable estimate for the timescale within which a response will be provided which will not exceed two (2) months from receipt of the data subject's notice of dispute. The Data Protection Team will keep evidence of data protection-related questions, concerns and complaints received from data subjects. Depending on the volume and nature of the complaints received, the DPO may review this Complaint Handling Procedure.

3.3.3 The Data Protection Team will provide a report to the Shopify's senior management team on an annual basis, which will include information on the complaints received, the subject of the complaints and the outcome of their handling.

3.3.4 If the complaint is upheld, the Data Protection Team will arrange for any necessary steps to be taken as a consequence. If the data subject is not satisfied with the outcome, they have the right to take the actions set out in paragraph 4 below.

4. Right of third party beneficiaries to complain to a competent supervisory authority and to commence proceedings

4.1.1 Where a data subject is conferred third party beneficiary rights under Part IV of the Controller Policy, then they will have certain additional rights to pursue effective remedies for their complaints, as described below.

4.1.2 These data subjects have the right to complain:

(a) to a competent supervisory authority in the European territory of the data subject's:

(i) habitual residence;

(ii) place of work; or

(iii) place of the alleged infringement; and/or

(b) to commence proceedings in a court of competent jurisdiction of:

(i) the European territory where the controller or processor has an establishment; or

(ii) where the data subject has their habitual residence.

4.1.3 Shopify accepts that complaints and claims made pursuant to paragraphs 4.1.2(a) and/or 4.1.2(b) may be lodged by a not-for-profit body, organisation or association acting on behalf of the data subjects concerned, to the extent such complaints and claims are permitted by relevant law.

4.1.4 If a data subject wishes to complain about Shopify's processing of his or her personal data to a European supervisory authority or to commence court proceedings against

Shopify, on the basis that a non-European group member has processed personal data in breach of the Controller Policy or in breach of applicable data protection laws, then Shopify International Limited will submit to the jurisdiction of the competent European supervisory authority or court, as applicable, in place of that non-European group member, as if the alleged breach had been caused by Shopify International Limited.

Appendix 8 - Cooperation Procedure

1. Background

1.1 Shopify's Binding Corporate Rules: Cooperation Procedure sets out the way in which Shopify will cooperate with competent supervisory authorities in relation to the Controller Policy.

2. Cooperation Procedure

2.1 Where required and upon request, Shopify will make necessary personnel available to a competent supervisory authority to discuss questions about or concerns with the Controller Policy.

2.2 Shopify will review, consider and (as appropriate) implement:

(a) any advice or decisions of relevant competent supervisory authorities on any data protection law issues that may affect the Controller Policy; and

(b) any guidance published by supervisory authorities (including the European Data Protection Board or any successor to it) in connection with Binding Corporate Rules for Controllers.

2.3 Shopify will upon request provide any information about the processing operations covered by the Controller Policy to a competent supervisory authority.

2.4 Shopify will upon request provide copies of the results of any audit it conducts of the Controller Policy to a competent supervisory authority.

2.5 Shopify agrees that a supervisory authority may audit the compliance with the Controller Policy of any group member for which it is competent in accordance with the applicable data protection law(s) of its jurisdiction.

2.6 Shopify agrees to abide by a decision of any competent supervisory authority on any issues relating to the interpretation and application of the Controller Policy (unless and

to the extent that Shopify is entitled to appeal any such decision and has chosen to exercise such right of appeal).

2.7 Shopify agrees that any dispute related to the competent supervisory authority's exercise of supervision of compliance with the Controller Policy will be resolved by the courts of the European country of that supervisory authority, in accordance with that European country's procedural law. The group members agree to submit themselves to the jurisdiction of these courts.

Appendix 9 - Updating Procedure

1. Introduction

1.1 This Binding Corporate Rules: Updating Procedure describes how Shopify must communicate changes to the Controller Policy to individual data subjects, to Shopify group members bound by the Controller Policy, and to competent supervisory authorities.

2. Records keeping

2.1 Shopify must maintain a change log which details each and every change made to the Controller Policy, including the nature of the change, the reasons for the change, the date the change was made, and who approved the change.

2.2 Shopify must also maintain an accurate and up-to-date list of group members that are bound by the Controller Policy. Shopify must provide this information upon request to competent supervisory authorities, and to data subjects who benefit from the Controller Policy.

2.3 The Data Protection Team shall be responsible for ensuring that the records described in this paragraph 2 are maintained and kept accurate and up-to-date.

3. Changes to the Controller Policy

3.1 The Data Protection Team will review and, where necessary, update Shopify's Controller Policy on a regular basis and in response to any relevant new developments, (for example changes to the scope of the BCR-C, the EDPB Recommendations or the regulatory environment), and to ensure that a high standard of protection is maintained for the data protection rights of data subjects who benefit from the Controller Policy. No changes to the Controller Policy shall take effect unless reviewed and approved by the Data Protection Team.

3.2 Shopify will communicate all changes to the Controller Policy (including reasons that justify the changes) or to the list of group members bound by the Controller Policy:

(a) to the group members bound by the Controller Policy via written notice (which may include e-mail or posting on an internal Intranet accessible to all group members);

(b) to the data subjects who benefit from the Controller Policy via the Shopify corporate website at https://www.shopify.com; and

(c) to the lead supervisory authority and any other relevant supervisory authorities the lead supervisory authority may direct, at least once a year. The lead supervisory authority should also be notified once per year in instances where no changes have been made to the Controller Policy.

4. Communication of material changes

4.1 If Shopify makes any material changes to the Controller Policy or to the list of group members bound by the Controller Policy that affect the level of protection offered by the Controller Policy or otherwise significantly affect the Controller Policy (for example, by making changes to the binding nature of the Controller Policy), it will promptly report such changes (including the reasons that justify such changes) to the lead supervisory authority.

5. Transfers to new group members

5.1 If Shopify intends to transfer personal data to any new group members under the Controller Policy, it must first ensure that all such new group members are bound by the Controller Policy before transferring personal data to them.

Appendix 10 - Government Disclosure Request Procedure

1. Introduction

1.1 This Binding Corporate Rules: Government Disclosure Request Procedure sets out Shopify's procedure (a) for responding to a request received from a law enforcement or state security body (together the "**Requesting Authority**") to disclose personal data processed by Shopify (hereafter "**Disclosure Request**") or (b) in the event it becomes aware of any other direct access by public authorities to personal data transferred pursuant to the Controller Policy in accordance with the laws of the country of destination. This Appendix relates to **Rule 10** and **commitment 11**. Government requests for disclosure of personal data of Part III of the Controller Policy.

1.2 Where Shopify receives a Disclosure Request, it will handle that Disclosure Request in accordance with this Procedure. If applicable data protection law(s) require a higher standard of protection for personal data than is required by this Procedure, Shopify will comply with the relevant requirements of applicable data protection law(s).

2. General Approach to Disclosure Requests

2.1 As a general principle, Shopify does not disclose personal data in response to a Disclosure Request unless either:

- it is under a compelling legal obligation to make such disclosure; or
- taking into account the nature, context, purposes, scope and urgency of the Disclosure Request and the privacy rights and freedoms of any affected data subjects, there is an imminent risk of serious harm that merits compliance with the Disclosure Request in any event.

2.2 In the event that Shopify is disclosing personal data in response to a Disclosure Request, the Shopify group member outside Europe agrees to provide the minimum amount of information permissible when responding to a Disclosure Request, based on a reasonable interpretation of the request. In no event will any group member transfer

personal data to a Requesting Authority in a disproportionate and indiscriminate manner that goes beyond what is necessary in a democratic society.

3. Handling of a Disclosure Request

3.1 Receipt of a Disclosure Request

3.1.1 If a Shopify group member outside Europe (i) receives a Disclosure Request or (ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to the Controller Policy in accordance with the laws of the country of destination, the Regulatory Affairs and Enforcement Team shall, on behalf of the Shopify group member, promptly inform:

(a) the Shopify group member exporting the data from Europe; and

(b) the data subject (where possible).

3.1.2 Such notification regarding a Disclosure Request should include, where available: details of the personal data requested, the requesting body, the legal basis for the request and the response provided, to the extent permitted by applicable law. A notification in respect of direct access by public authorities to personal data transferred pursuant to the Controller Policy should include information available to the Shopify group member outside Europe.

3.1.3 If the Shopify group member outside Europe is prohibited from notifying the Shopify group member exporting the data from Europe, the data importer will use its best efforts to obtain a waiver of such prohibition, with a view to communicating as much information as possible and as soon as possible, and will document its best efforts in order to be able to demonstrate them upon request of the data exporter.

3.2 Initial steps

3.2.1 Shopify's Regulatory Affairs and Enforcement Team, acting on behalf of the Shopify group member in receipt of the Disclosure Request, will carefully review each and every Disclosure Request on a case-by-case basis to determine the nature, context, purposes,

scope, urgency, and validity of the Disclosure Request under the laws of the country of destination, notably whether it remains within the powers granted to the Requesting Authority, in order to identify whether action may be needed to challenge the Disclosure Request. Shopify's Regulatory Affairs and Enforcement Team will review possibilities to appeal the Disclosure Request if, after careful assessment, it concludes that the Disclosure Request is unlawful under the laws of the country of destination and applicable obligations under international law. When challenging a request, the Regulatory Affairs and Enforcement Team shall seek interim measures with a view to suspending the effects of the Disclosure Request until the court has decided on the merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are notwithstanding the obligations of the Shopify group member pursuant to **commitment 10**. Conflicts between this Controller Policy and national legislation of Part III of the Controller Policy (i.e. the obligation to notify the DPO if it has reason to believe that it cannot comply with the Controller Policy).

3.2.2 The Shopify group member outside Europe agrees to document its legal assessment as well as any challenge to the Disclosure Request and, to the extent permissible under the laws of the country of destination, make such assessment available to the Shopify group member exporting the data from Europe. It shall also make a non-privileged summary of this assessment available to any Supervisory Authority on request.

4. Notice of a Disclosure Request

4.1 Notice to the Data Subject

4.1.1 If a request concerns personal data for which Shopify is the controller, Shopify will notify and provide the data subject(s) with details of the Disclosure Request prior to disclosing any personal data, unless (i) legally prohibited; (ii) an imminent risk of serious harm exists that prohibits prior notification; or (iii) such notification is not reasonably possible.

4.2 Notice to Shopify group member exporting the personal data

4.2.1 Shopify's Regulatory Affairs and Enforcement Team, acting on behalf of the Shopify group member importing the personal data, will provide the group member exporting the personal data with as much relevant information as possible on the request received (e.g. the number and type of Disclosure Requests, the jurisdiction of the Requesting Authorities who made those requests, the type of data requested, whether requests have been challenged and the outcome of such challenges, etc.). If the group member importing the personal data becomes partially or completely prohibited from providing the data exporter with this information it will inform the group member exporting the personal data of this without delay.

4.3 The Shopify group member importing the personal data agrees to preserve this information for the duration of the processing of personal data and make a non-privileged summary of this information available to any Supervisory Authority upon request.

Appendix 11 – Transfer Risk Assessment

1. Background

1.1 Shopify's Controller Policy protects the personal data transferred between Shopify group members.

2. Transfer Risk Assessment

2.1 This Appendix relates to **Rule 11** and **commitment 10** of Part III of the Controller Policy and sets out the elements that should be considered when undertaking a transfer risk assessment:

2.2 the specific circumstances of the transfer, including:

(a) the type of recipients;

(b) economic sector in which the transfer occurs;

(c) the purpose of processing;

(d) the categories and format of the personal data;

(e) the location of the processing, including storage; and

(f) the transmission channels used.

2.3 the laws and practices of the country in which the group member is established in light of the circumstances of the transfer, including those requiring to disclose data to public authorities or authorising access by such authorities, as well as the applicable limitations and safeguards; and

2.4 any safeguards in addition to those under the Controller Policy, including the technical and organisational measures applied during transmission and to the processing of the personal data in the country of destination in which the group member is established.

Appendix 12 – Material Scope of the Controller Policy

1. **Background**

1.1 Shopify's Controller Policy provides a framework for the transfer of personal data between Shopify group members.

1.2 This document sets out the material scope of the Controller Policy. It specifies the data transfers or set of transfers, including the nature and categories of personal data, the type of processing and its purposes, and the types of data subjects affected.

2. **Human resources data**

Who transfers the personal data described in this section?	Every Shopify group member inside of Europe may transfer the personal data that they control described in this section to every other Shopify group member inside and outside of Europe. Every group member outside of Europe may also transfer the personal data that they control described in this section to every Shopify group member inside and outside of Europe.
Who receives this personal data?	Every Shopify group member outside of Europe may receive the personal data described in this section which is sent to them by other Shopify group members inside and outside of Europe. Every group member inside of Europe may also receive the personal data described in this section which is sent to them by other Shopify group members inside and outside of Europe.

What categories of personal data are transferred?	Personal data relating to past and current employees, consultants, independent contractors, temporary staff, and job candidates. Specifically includes (if applicable): ● contact information, including home address, telephone number, and email address; ● government identifiers, such as social insurance number, social security number, or taxpayer identifier number; ● benefits information, such as about sick pay, bank accounts, information about dependents and beneficiaries if we extend benefits to them, emergency contacts, clothing sizes to provide promotional clothing, physical limitations, or special needs to provide work accommodations; ● demographic information, such as age, gender, marital status and nationality, gender identity, ethnic or racial background, disability, political affiliation, caregiver status, or sexual orientation to promote equality and diversity at Shopify; ● employment information, such as promotions history, salary history, work appraisals, performance improvement plans, time off, disciplinary history, past employment history, legal eligibility to work; ● access records of employee access to and use of Shopify's platform, Shopify-owned or Shopify-managed devices, and internal applications;

	● information captured through office security systems, such as CCTV and access control entry systems; ● results of criminal and credit background checks; or ● information received from third parties, including information we receive as part of a legal or regulatory process.
What categories of special categories of personal data (if any) are transferred?	Personal data revealing racial or ethnic origin, data concerning health, or data concerning a natural person's sex life or sexual orientation.
Who are the types of data subjects whose personal data are transferred?	Past and current employees, consultants, independent contractors, temporary staff, and job candidates.
Why is this personal data transferred and how will it be used?	HR data is transferred for the purposes of global staff administration; the management of training; payroll and benefit administration; recruitment and performance management; compliance with mandatory reporting obligations and other regulatory requirements; the operation of internal global staff contact directories; and emergency contact; provision of resources; to investigate and respond to complaints, inquiries, and legal claims; to evaluate and improve hiring and employment practices, including with respect to diversity and inclusion; data storage; and to protect Shopify, Shopify's property, Shopify's customers, and other employees and contractors from threats.
Where is this personal data processed?	The personal data described in this section may be processed in every territory where Shopify group members

	or their processors are located. A list of Shopify group member locations is available in **Appendix 1** – Shopify Group Members .

3. **Merchant data**

Who transfers the personal data described in this section?	Every Shopify group member inside of Europe may transfer the personal data that they control described in this section to every other Shopify group member inside and outside of Europe. Every group member outside of Europe may also transfer the personal data that they control described in this section to every Shopify group member inside and outside of Europe.
Who receives this personal data?	Every Shopify group member outside of Europe may receive the personal data described in this section which is sent to them by other Shopify group members inside and outside of Europe. Every group member inside of Europe may also receive the personal data described in this section which is sent to them by other Shopify group members inside and outside of Europe.
What categories of personal data are transferred?	Personal data relating to merchants or representatives of merchants who use Shopify's services. Specifically includes (if applicable): name, company name, staff name(s), mailing address, email address, phone number, payment card information, bank account number, device information, IP address, business ID or registration number, date of birth, government-issued identification,

	Social Security Number, Social Information Number, Employer Identification Number, or Tax Identification Number, picture of self with ID card, event attendance information, personal data provided in order to provide customer support.
What categories of special categories of personal data (if any) are transferred?	If disclosed voluntarily by the merchant, Shopify collects personal data revealing the racial or ethnic origin or sexual orientation of the business owner, for the purposes of promoting diverse businesses.
Who are the types of data subjects whose personal data are transferred?	Merchants or representatives of merchants who use Shopify's services.
Why is this personal data transferred and how will it be used?	Merchant data is transferred for the purposes of providing the Shopify services, data storage, transfer to processors, to comply with legal requirements, to bill for Shopify's services, to improve Shopify's platform and services, to personalise Shopify's services, to advertise and market products and features, to conduct fraud and risk monitoring, to verify account ownership, to provide customer service, and to provide tax documentation.
Where is this personal data processed?	The personal data described in this section may be processed in every territory where Shopify group members or their processors are located. A list of Shopify group member locations is available in **Appendix 1** – Shopify Group Members.

4. **Partner data**

Who transfers the personal data described in this section?	Every Shopify group member inside of Europe may transfer the personal data that they control described in this section to every other Shopify group member inside and outside of Europe. Every group member outside of Europe may also transfer the personal data that they control described in this section to every Shopify group member inside and outside of Europe.
Who receives this personal data?	Every Shopify group member outside of Europe may receive the personal data described in this section which is sent to them by other Shopify group members inside and outside of Europe. Every group member inside of Europe may also receive the personal data described in this section which is sent to them by other Shopify group members inside and outside of Europe.
What categories of personal data are transferred?	Personal data relating to Shopify partners and app developers who provide services or develop technology for merchants in connection with their use of Shopify's technology. This includes (if applicable): name, company name, email address, mailing address, phone number, payment card number or bank account number, device information, browser information, details about how a partner browses through Shopify's apps and sites, IP address, government-issued identification.

What categories of special categories of personal data (if any) are transferred?	N/A
Who are the types of data subjects whose personal data are transferred?	Shopify partners and app developers who provide services or develop technology for merchants in connection with their use of Shopify's technology.
Why is this personal data transferred and how will it be used?	Managing the business relationship, data storage, and record-keeping purposes.
Where is this personal data processed?	The personal data described in this section may be processed in every territory where Shopify group members or their processors are located. A list of Shopify group member locations is available in **Appendix 1** – Shopify Group Members.

5. **Customer data**

Who transfers the personal data described in this section?	Every Shopify group member inside of Europe may transfer the personal data that they control described in this section to every other Shopify group member inside and outside of Europe. Every group member outside of Europe may also transfer the personal data that they control described in this section to every Shopify group member inside and outside of Europe.
Who receives this personal data?	Every Shopify group member outside of Europe may receive the personal data described in this section which is

	sent to them by other Shopify group members inside and outside of Europe. Every group member inside of Europe may also receive the personal data described in this section which is sent to them by other Shopify group members inside and outside of Europe.
What categories of personal data are transferred?	Customer data includes: (i) personal data relating to end users of Shopify's customer-facing applications and services (including Shopify's corporate website or other online properties); and (ii) personal data relating to merchant customers for the development and provision of Enhanced Services (as defined in section 9.2 of Shopify's Terms of Service). This includes (as applicable): name, email address, phone number, shipping address, payment card number or bank account number, information from email messages in the email inboxes that are connected to a user's Shop account, order history, use of certain Shopify apps and services, shopping service integrations, device information, device location, IP address, government-issued identification, activity with Shopify merchants.
What categories of special categories of personal data (if any) are transferred?	N/A
Who are the types of data subjects whose personal data are transferred?	Customers who: (i) use Shopify's customer-facing applications and services, such as Shop Pay and Shop (including Shopify's corporate website or other online properties); or (ii) browse or shop on merchant's stores

	where merchants share this data with Shopify as a controller for the development and provision of Enhanced Services.
Why is this personal data transferred and how will it be used?	Customer data is transferred for the purposes of: (i) providing or providing support related to Shopify's custo mer-facing products and websites; and (ii) Shopify developing and providing specific services to merchants, such as Shop channel, Shopify Messaging, Shopify Search & Discovery, and Shopify Collabs. .
Where is this personal data processed?	The personal data described in this section may be processed in every territory where Shopify group members or their processors are located. A list of Shopify group member locations is available in **Appendix 1** – Shopify Group Members.

6. **Vendor data**

Who transfers the personal data described in this section?	Every Shopify group member inside of Europe may transfer the personal data that they control described in this section to every other Shopify group member inside and outside of Europe. Every group member outside of Europe may also transfer the personal data that they control described in this section to every Shopify group member inside and outside of Europe.
Who receives this personal data?	Every Shopify group member outside of Europe may receive the personal data described in this section which is sent to them by other Shopify group members inside and outside of Europe.

	Every group member inside of Europe may also receive the personal data described in this section which is sent to them by other Shopify group members inside and outside of Europe.
What categories of personal data are transferred?	Vendor personal data is personal data of individual contractors and of account managers and staff of third parties who provide services to us. Specifically includes (if applicable): business contact information such as name, phone number, email address, company mailing address.
What categories of special categories of personal data (if any) are transferred?	N/A
Who are the types of data subjects whose personal data are transferred?	Individual contractors, app developers, theme developers, and account managers and staff of third party suppliers who provide services to Shopify.
Why is this personal data transferred and how will it be used?	Partner and vendor data is transferred for the purposes of managing the business relationship with partners and vendors and for record-keeping purposes, and for the purpose of data storage.
Where is this personal data processed?	The personal data described in this section may be processed in every territory where Shopify group members or their processors are located. A list of Shopify group member locations is available in **Appendix 1** – Shopify Group Members.

Appendix 13 – Legal Justification for Data Processing

1. **Background**

1.1 Shopify's Controller Policy provides a framework for the transfer of personal data between Shopify group members.

1.2 This document outlines the legal bases we intend to rely on for the processing of personal data.

2. Human resources data

2.1 Human resources data includes the personal data of past and current employees, individual consultants, independent contractors, temporary staff and job applicants.

2.2 Human resources data legal justification table

Types of information	Legal justification
Contact information (e.g. name, personal address, telephone number, and email address)	● Employees: Legitimate interest in enabling employees to carry out their duties; Performance of a contract ● Candidates: Pre-contractual necessity; Legitimate interest in communicating with potential candidates
Payment information such as bank account details	● Contractual necessity
Information contained in resumes, cover letters and applications	● Legitimate interest in protecting the security of our business and ensuring a safe place of work ● Legitimate interest in determining the skills and qualifications of a candidate
HR files and records of employment	● Performance of contractual obligations

	● Legitimate interest of Shopify to manage its employees ● Legitimate interest in protecting the security of our business and ensuring a safe place of work

3. Merchant data

3.1 Merchant data includes personal data relating to representatives or agents of merchants who use Shopify's business services and Shopify Payments.

3.2 Merchant data legal justification table

Types of information	Legal justification
Business information e.g. merchants name and contact details, the name of staff or other individuals associated with the merchants business, company name, address, email address, and phone number	● Contractual necessity ● Legitimate interests to improve our products and services, provide advertise and market our products and features, prevent fraud, and provide an appropriate level of merchant support ● Comply with our legal obligations e.g. compliance with tax or law enforcement obligations ● Consent for certain marketing and advertising purposes
Payment information e.g. merchant's payment card details, bank account information, and for those merchants using Shopify Capital, we also collect information about the business's bank accounts or financial assets.	● Contractual necessity ● Legitimate interests to improve our products and services, provide, advertise, and market our products and features, prevent fraud, and

	provide an appropriate level of merchant support ● Comply with our legal obligations e.g. compliance with tax or law enforcement obligations
Information about how merchants access Shopify websites, their account, and Shopify's platform, including device and browser information, network connection, IP address, and browsing information, including information by using cookies.	● Contractual necessity ● Legitimate interest to improve our products and services, to protect the safety and security of our products and services and to detect and prevent fraud ● Consent for certain marketing and advertising purposes
For merchants using Shopify Payments, information merchants provide us including their business address, business type, business ID number, bank account information, date of birth (if they are an individual business owner), and in some circumstances, government-issued identification.	● Contractual necessity ● Legitimate interests to improve our products and services, prevent fraud, and provide an appropriate level of merchant support ● Comply with our legal obligations e.g. compliance with tax or law enforcement obligations
Identity information e.g. copies of government-issued identity documentation	● Contractual necessity ● Legitimate interest in providing an appropriate level of merchant support ● Comply with our legal obligations e.g. compliance with tax or law enforcement obligations
Data revealing the racial or ethnic origin of the business owner	● Consent for certain diversity initiatives

4. Customer data

4.1 Customer data is data collected from individuals who (i) use Shopify's customer facing applications and services (including Shopify's corporate website or other online properties); or (ii) browse or shop with merchants on merchant's stores where merchants share this data with Shopify as a controller for the development and provision of Enhanced Services.

4.2 Customer data legal justification table

Types of information	Legal justification
Profile and contact information e.g. name, address, email address, billing address, shipping address, phone number, identity documents.	● Contractual necessity ● Legitimate interest to improve our products and services ● Comply with our legal obligations e.g. compliance with tax or law enforcement obligations ● Consent for certain marketing and advertising purposes
Device information about the devices used to interact with Shopify, Shopify merchants, and/or the Shopify Consumer Services, including IP address, device identifiers, cookie IDs, browser, network connection, or other unique identifiers or device information.	● Contractual necessity ● Legitimate interest to improve our products and services ● Comply with our legal obligations e.g. compliance with tax or law enforcement obligations ● Consent for certain marketing and advertising purposes
Payment information e.g. payment card number and expiration date.	● Contractual necessity
Use of Shopify apps and services including interactions with Shopify merchants in the Shop app, the shops visited and purchased	● Contractual necessity

from, products viewed and purchased, product reviews and ratings, order history, purchases using Shop Pay, search queries, favorited shops and other activities related to the Shopify Consumer Services.	● Legitimate interest to improve our products and services ● Comply with our legal obligations e.g. compliance with tax or law enforcement obligations ● Consent for certain marketing and advertising purposes
Activity with Shopify merchants including activity information on Shopify merchant site, including browsing and search activity, shopping and purchase activity, billing and shipping information, transaction details and payment information.	● Contractual necessity ● Legitimate interest to improve our products and services ● Comply with our legal obligations e.g. compliance with tax or law enforcement obligations ● Consent for certain marketing and advertising purposes
Information about customer's settings and preferences on Shopify and our Merchants, as well as information about their browser and device privacy settings.	● Legitimate interest to provide such functionality customers ● Comply with our legal obligations e.g. compliance with data protection lawsC
Information concerning communication with Shopify e.g. customer support inquiries, taking surveys, participating in promotions or research.	● Contractual necessity ● Legitimate interest to provide this functionality, and improve our products and services
Limited information from customer social network accounts where they choose to link, connect, or login to Shopify Consumer Services through such a third party service.	● Contractual necessity ● Legitimate interest to provide this functionality, and improve our products and services
Information from email messages in the inboxes that customers connect to their Shop account, and information from email	● Contractual necessity

messages they transfer to the Shop app to be included in their order history.	● Legitimate interest to provide this functionality, and improve our products and services ● Consent

5. Partner and vendor data

5.1 Partner and vendor data includes the personal data of individual contractors, app developers, theme developers, value-add partners, creators, and of account managers and staff of third party suppliers who provide services to Shopify.

5.2 Partner and vendor data legal justification table

Types of Information	Legal Justification
Contact information (company name, company address, telephone number, and email address)	● Contractual necessity ● Legitimate interests in providing advertising that is relevant to partners' interests ● Consent from partners for certain marketing and advertising purposes
Payment information (such as credit / debit card information, bank account number)	● Contractual necessity
Information about how a partner accesses and uses Shopify apps, websites, and other services, including device information, browser information, information on network connection, IP address, communication with merchants and details about how a partner browses through our apps and sites	● Contractual necessity ● Our legitimate interest to improve our products and services, protect the safety and security of our products and services and to detect and prevent fraud
Copies of Government-issued I.D. a partner provides	● Contractual necessity

	● Comply with our legal obligations e.g. compliance with tax or law enforcement obligations