Shopify

Binding Corporate Rules:

Processor Policy

Contents

Part I: Introduction

This Binding Corporate Rules: Processor Policy ("Processor Policy") applies when Shopify processes personal data as a processor on behalf of a third party controller and transfers such personal data between group members. This Processor Policy applies regardless of whether our group members process personal data by manual or automated means.

This Processor Policy applies to transfers of personal data made by Shopify when acting as a processor on behalf of a third party controller (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 Processor Policy, like "controller", "processor", and "personal data", please see the section titled "Important terms used in this Processor Policy" below.

Types of personal data within the scope of this Processor Policy

This Processor Policy applies to all personal data that we process as a processor on behalf of a third party controller (referred to as the "**Merchant**" in this Processor Policy), such as:

- personal data relating to a Merchant's customers who visits or makes purchases through a Merchant store that uses Shopify's platform or services. This will include, for example, information about the customer's name, contact information, shipping information, details regarding the items or services purchased, and, if the Merchant uses Shopify as a payment processor, payment information.

- information related to a Merchant's customer that a Merchant directly provides to Shopify in relation to the services (such as order information, customer lists, etc.) to the extent that they include any personal data.

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

Our collective responsibility to comply with this Processor Policy

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

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

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

Responsibility towards the Merchant

As a data processor, Shopify will have a number of direct legal obligations under applicable data protection laws. In addition, however, the Merchant will also pass certain data protection obligations on to Shopify in its contract appointing Shopify as its processor. If Shopify fails to comply with the terms of its contract, this may put the Merchant in breach of its applicable data protection laws and Merchant may bring a legal claim against Shopify for breach of contract, resulting in the payment of compensation or other judicial remedies as set out in the relevant contract.

A Merchant may enforce this Processor Policy against any group member that is in breach of it. Where a non-European group member (or a non-European third party processor appointed by a group member) processes personal data about a data subject for which the Merchant is a controller in breach of this Processor Policy, that Merchant may enforce the Processor Policy against Shopify International Limited. In such an event, Shopify International Limited will be responsible for demonstrating that such group member (or third party processor) is not responsible for the breach, or that no such breach took place.

When a Merchant transfers personal data to a group member for processing in accordance with this Processor Policy, this Processor Policy shall be incorporated into the contract with that

Merchant by means of a specific reference to it and shall be made binding towards the Merchant. If a Merchant chooses not to rely upon this Processor Policy when transferring personal data to a group member outside Europe, that Merchant is responsible for implementing other appropriate safeguards in accordance with applicable data protection laws.

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 Processor 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 Processor Policy.

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

Relationship with Shopify's Binding Corporate Rules: Controller Policy

This Processor Policy applies only to personal data that Shopify processes as a processor in order to provide a service to a Merchant. Shopify has a separate Binding Corporate Rules: Controller Policy ("**Controller Policy**") that applies when it processes personal data as a controller (i.e. for its own purposes). When a Shopify group member processes personal data as a controller, it must comply with the Controller 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, please speak with Shopify's Data Protection Team whose contact details are provided below.

Where will this Processor Policy be made available?

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

Important terms used in this Processor Policy

For the purposes of this Processor 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 in which the controller of the personal data is located. Where a group member processes personal data on behalf of a European controller under this Processor Policy, the term applicable data protection laws shall include the European data protection laws applicable to that controller (including the General Data Protection Regulation (as defined below));

- the term **binding corporate rules** or **BCRs** means this set of Binding Corporate Rules for Processors 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 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, in certain instances Shopify is a processor of the personal data of Merchants' customers in the provision of Shopify's services to its Merchants);

- 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 Processor 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 terms **we** or **our** refer to the Shopify group of entities.

How to raise questions or concerns

If you have any questions regarding this Processor Policy, your rights under this Processor 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 Processor 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 Processor Policy applies in all situations where a group member processes personal data as a processor 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 law and this Processor Policy.***	We must at all times comply with any applicable data protection laws, as well as the standards set out in this Processor Policy, when processing personal data. We must only process personal data on behalf of the Merchant and in accordance with the Merchant's documented instructions (for example, as set out in the terms of our contract with the Merchant). As such: ● where applicable data protection laws exceed the standards set out in this Processor 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 Processor Policy, we must process personal data in accordance with the standards set out in this Processor Policy.
Rule 2 – Fairness and transparency: ***We must, to the extent reasonably possible, help a Merchant comply with the requirement to explain to data subjects how their personal data will be processed.***	A Merchant has a duty to explain to the data subjects whose information it processes (or instructs us to process), how and why that information will be used. This information must be given in a concise, transparent, intelligible and easily accessible form, using clear and plain language. This is usually done through an easily accessible privacy policy or fair processing statement. We will provide such assistance

	and information to the Merchant in accordance with the terms of our contract with the Merchant to comply with this requirement. For example, the terms of our contract with a Merchant may require us to provide information about any sub-processors we appoint to process personal data on our Merchant's behalf.
Rule 3 – Cooperation with Merchants: ***We must, to the extent reasonably possible, cooperate with and help a Merchant comply with its obligations under applicable data protection laws.***	We must cooperate with and help a Merchant comply with its obligations under applicable data protection laws. We must provide such assistance in a reasonable time and to the extent reasonably possible, and as required under the terms of our contract with the Merchant. Assistance may include, for example, helping a Merchant (such as by providing a means by which the Merchant can access and directly edit personal data) to keep the personal data we process on its behalf accurate and up to date, helping it to provide data subjects with access to their personal data, providing sufficient information in order to help the Merchant to conduct data protection impact assessments in accordance with applicable data protection laws, and being in a position to help the Merchant reply to an investigation or inquiry from supervisory authorities.
Rule 4 – Purpose limitation: ***We will only process personal data on behalf of, and in accordance with the instructions of, the Merchant.***	We must only process personal data on behalf of the Merchant and in accordance with the Merchant's documented instructions (for example, as set out in the terms of our contract with the Merchant).

	If we are unable to comply with a Merchant's instructions (or any of our obligations under this Processor Policy), we will promptly inform the Merchant. The Merchant may then suspend its transfer of personal data to us and/or terminate its contract with us (in accordance with the terms of the contract). In such circumstances, we will return or delete the personal data, including any copies of the personal data, in a secure manner or as otherwise required, in accordance with the terms of our contract with the Merchant. Shopify will also comply with the above when the contract between us and the Merchant terminates. If we are prevented from returning the personal data to a Merchant, or from deleting it (for example, due to applicable law requirements), we must inform the Merchant. In such an event, we will maintain the confidentiality of the personal data and not process the personal data further, other than in accordance with the terms of our contract with the Merchant.
Rule 5 – Data accuracy and minimisation: ***We will help a Merchant keep the personal data accurate and up to date***	We must help a Merchant comply with its obligation to keep personal data accurate and up to date. In particular, where a Merchant informs us that personal data is inaccurate, we must enable a Merchant to update, correct or erase that information without delay. In such circumstances, we must also take measures to inform group members or third party processors to whom the personal data has been disclosed of the need to update, correct or erase that personal data.

Rule 6 – Storage limitation: ***We will help our Merchant store personal data only for as long as is necessary for the purpose for which the data was initially collected.***	Where a Merchant instructs us that personal data we process on its behalf is no longer needed for the purposes for which it was collected, we will help our Merchant erase or anonymise that personal data without delay and in accordance with the terms of our contract with the Merchant. In such circumstances, we must also take measures to inform group members or third party processors to whom the personal data has been disclosed of the need to erase, restrict or anonymise that personal data.
Rule 7 – Security, integrity and confidentiality: ***We must implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk to the personal data we process on behalf of a Merchant.***	Where we provide a service to a Merchant which involves the processing of personal data as a processor, the contract between us and that Merchant will set out the technical and organisational measures we must implement to safeguard that information consistent with applicable data protection laws. We must implement appropriate technical and organisational measures organisational measures to: (i) ensure and to be able to demonstrate that processing is performed in accordance with the BCRs; 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. We must ensure that any staff member who has access to personal data processed on behalf of a Merchant does so only

	for purposes that are consistent with the Merchant's instructions and is subject to a duty of confidence.
Rule 8 – Security incident reporting: ***We must notify a Merchant of any security incident that we experience if it presents a risk to the personal data we process on the Merchant's behalf.***	When we become aware of a data security incident that presents a risk to the personal data that we process on behalf of a Merchant, the Data Protection Team will follow our security incident management policies. The Data Protection Team will review the nature of the data security incident and will notify the Merchant where required (according to the terms in place with the Merchant). The Data Protection Team shall be responsible for ensuring that any such notifications are made without undue delay after becoming aware of the personal data breach and in accordance with applicable data protection law.
Rule 9 – Engaging sub-processors ***We may only appoint, add or replace sub-processors with the authorisation of the Merchant.***	We must obtain a Merchant's general authorisation to the appointment of sub-processors to process personal data on its behalf in our contract with the Merchant. We must inform the Merchant in a timely manner (such that the Merchant has a possibility to object) of any intended changes concerning the addition or replacement of a sub-processor. If, on reviewing this information, a Merchant objects to the appointment of a sub-processor, that Merchant may take such steps as are consistent with the terms of its contract with us and as referred to in **Rule 4** of this Processor Policy regarding the return or destruction of the personal data.

Rule 10 – Sub-processor contracts ***We must only appoint external sub-processors who protect personal data to a standard that is consistent with this Processor Policy and our contractual terms with Merchants.***	We must only appoint sub-processors who provide sufficient guarantees in respect of the commitments made by us in this Processor Policy. In particular, sub-processors must implement appropriate technical and organisational security measures to protect the personal data they process, to the same standard as our commitments to a Merchant under our contractual terms with the Merchant. Where we intend to appoint an external sub-processor to process personal data, we must undertake due diligence to ensure it has in place appropriate technical and organisational security measures to protect the personal data. We must impose in writing strict contractual obligations on the sub-processor that require it: ● to protect the personal data to a standard that is consistent with our commitments to a Merchant under the terms of our contract with the Merchant; ● to maintain the security of the personal data, consistent with standards contained in this Processor Policy (and in particular Rules 7, 8 and 9 above); ● to process personal data only on our instructions (which instructions will be consistent with the instructions of the Merchant) or on the Merchant's instructions; and ● to fulfil such additional obligations as may be necessary to ensure that the commitments made by the sub-processor reflect those made by us in this Processor Policy, and which, in particular, provide for adequate safeguards with respect to the privacy and fundamental rights and freedoms of data subjects in respect of any transfers of personal data.

Rule 11 – Respect for data subjects' data protection rights: ***We will help a Merchant respond to queries or requests made by data subjects in connection with their personal data.***	We must help a Merchant comply with its duty to respect the data protection rights of data subjects, in accordance with the instructions of the Merchant and the terms of our contract with the Merchant. In particular, if any group member receives a request from any data subject wishing to exercise his or her data protection rights over personal data for which the Merchant is the controller, the group member must direct such request within a reasonable timeframe to the relevant Merchant and not respond to such a request unless authorised to do so or required by law (in accordance with the Data Protection Rights Procedure in **Appendix 3**).

Rule 12 - Ensuring adequate protection for transfers: ***We must not transfer personal data without ensuring adequate protection for the data in accordance with applicable data protection law***	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 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 these BCRs intends to onward transfer that personal data to sub-processors that are not bound by the BCRs. Any such personal data that have been transferred under these BCRs may only be onward transferred outside Europe to sub-processors which are not bound by the BCRs 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 individual 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 individual and the controller or the implementation of pre-contractual measures taken at the individual's request, iii) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the controller and another natural or legal person, iv) the transfer is necessary for important reasons of public interest, 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 individual or of other persons, where the individual 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 these BCRs 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 these BCRs. 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 these BCRs. The group member shall in providing this assurance take into account the elements set out in **Appendix 11** (Transfer Risk Assessment). 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 these BCRs. The group members involved in the transfer agree to document this assessment, as well as any supplementary measures, 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 these BCRs, 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 these BCRs cannot be adhered to and more specifically that the requirements contained in these BCRs 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 BCRs. The group member importing the data shall also notify the Data Protection Officer ("**DPO**") and Shopify International Limited of this fact in accordance with **commitment 9** of Part III. 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 these BCRs, 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 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.

Part III: Compliance in practice

To ensure we follow the rules set out in this Processor 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 Processor Policy. The Data Protection Team will work with other relevant teams to oversee and enable compliance with this Processor 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 Processor 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 data processing activities carried out on behalf of a Merchant.***	We must maintain a record of the processing activities that we conduct on behalf of a Merchant in accordance with applicable data 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 processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the DPO; (ii) the categories of processing carried out on behalf of each controller; (iii) 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), the documentation of suitable safeguards; (iv) where possible, a general description of the technical and organisational security measures referred to in Article 32(1). The Data Protection Team is responsible for ensuring that such records are maintained.

4. Audit: ***We must conduct data protection audits on a regular basis.***	We will conduct data protection audits to verify compliance with all aspects of these BCRs by group members (including methods and action plans 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 Processor Policy. After each audit, the data protection audit reports will be submitted to the DPO to the board of directors of Shopify International Limited, and potentially 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 BCRs 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, in some circumstances.

	We will conduct any such audits in accordance with the Audit Protocol (see **Appendix 6**).
5. Data protection by design and by default: ***We must provide our products and services in a way that helps our Merchants implement the principles of data protection by design and data protection by default.***	We must provide our products and services in a way that helps our Merchants implement the principles of data protection by design and data protection by default. This means that we must implement appropriate technical and organisational measures when providing our products and services 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**"). These measures must be implemented in accordance with the terms of our agreement with our Merchants.
6. 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 Processor Policy) in accordance with the Complaint Handling Procedure (see **Appendix 7**).

7. 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**).
8. Updates to this Processor Policy: ***We will update this Processor Policy in accordance with our Updating Procedure***	We must update our Processor Policy in accordance with the Updating Procedure (see **Appendix 9**).
9. Conflicts between this Processor 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 material obligations under the Processor Policy or otherwise have a substantial effect on its ability to comply in all material respects with the Processor 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 Processor 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 **commitment 10** of this Part III. **9.1 Transparency when legislation prevents compliance with the BCRs** 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 authorising access by a public authority) prevent the group member from fulfilling its obligations under the BCRs. 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 material obligations under, or otherwise have a substantial, adverse effect on the guarantees provided by the BCRs (including the obligation to comply with the instructions of the Merchant), the group member shall, unless prohibited by law, promptly inform the exporting group member, the DPO and the Data Protection Team, who will make a responsible decision on the action to take and comply with the procedure in **Appendix 10** (Government Disclosure Request Procedure) and who will inform the Merchant. Where required, 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. Upon being informed in accordance with this section, the Merchant may then suspend its transfer of personal data to us and/or terminate its contract with us (in accordance with the terms of the contract). 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 and indiscriminate in a manner that would go beyond what is necessary in a democratic society. **9.2 Relationship between national laws and BCRs** Group members must process personal data in accordance with the BCRs. Where the national legislation requires a

	higher level of protection for personal data, such national legislation shall take precedence over these BCRs. 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 authorising access by public authorities) prevent the group member from fulfilling its obligations under the BCRs. In giving this assurance, each relevant group member has undertaken an assessment in particular considering the elements set out in **Appendix 11** (Transfer Risk Assessment) and has documented this assessment. Shopify will make available a non-privileged summary of this assessment to a supervisory authority on request. The elements to be considered in giving the assurance are set out at **Appendix 11**. 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 BCRs, 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 9.1** Transparency when legislation prevents compliance with the BCRs 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 9.1** Transparency when legislation prevents compliance with the BCRs 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 BCRs it shall comply with the procedure in **Appendix 10** (Government Disclosure Request Procedure).
10. Government requests for disclosure of personal data: ***We must comply with the 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 Processor Policy, it must comply with the Government Disclosure Request Procedure set out in **Appendix 10**.

11. Termination	In the event that a group member acting as data importer ceases to be bound by these BCRs, 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.
12. Non-Compliance	Shopify will ensure that no transfer is made to a group member unless the group member is effectively bound by the Processor 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 Processor Policy, for whatever reason, including the situations further described under **commitment 9** of Part III of this Processor 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 Processor 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 Processor Policy in its entirety, where: ● the group member exporting the personal data has suspended the transfer, and compliance with this Processor 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 Processor 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 Processor 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 third-party controller or a group member (acting as processor) established in Europe;
- a non-European Merchant (acting as controller) or group member (acting as processor) offers goods and services (including free goods and services) to those data subjects in Europe; or
- a non-European Merchant (acting as controller) or group member (acting as processor) monitors the behaviour of those data subjects, as far as their behaviour takes place in Europe;

and that Merchant or group member (as applicable) then transfers those data subjects' personal data to a non-European group member (or its sub-processor) for processing under the Processor 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 Processor Policy:

- Part I (Introduction) of this Processor Policy;
- Part II (Our Obligations) of this Processor Policy;
- Paragraphs 5 (Data protection by design and by default), 6 (Complaint Handling), 7 (Cooperation with Competent Supervisory Authorities), 9 (Conflicts between this Processor Policy and national legislation) and 10 (Government requests for disclosure of personal data) under Part III of this Processor Policy; and

- Part IV (Third Party Beneficiary Rights) of this Processor Policy.

Data subjects' third party beneficiary rights

When this Part IV applies, the right for data subjects to pursue effective remedies against Shopify apply only if (i) the requirements at stake are specifically directed at Shopify as a processor in accordance with applicable data protection law (and in accordance with the guidance published by competent supervisory authorities), and/or (ii) the data subjects cannot bring a claim against a Merchant because:

- the Merchant has factually disappeared or ceased to exist in law or has become insolvent; and

- no successor entity has assumed the entire legal obligations of the Merchant by contract or by operation of law that would allow the data subjects to enforce their rights against such a successor entity.

In such cases, 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 Processor 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 Processor 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 Processor Policy upon request to Shopify's Data Protection Team. A copy of the Processor Policy will also be made available online on Shopify's website at www.shopify.com/legal.

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 the Processor Policy by a non-European group member (or any non-European sub-processor appointed by a group member).

In particular:

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

- where a non-European group member (or any non-European third party sub-processor acting on behalf of a group member) fails to comply with this Processor 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 Processor Policy.

Shared liability for breaches with controllers

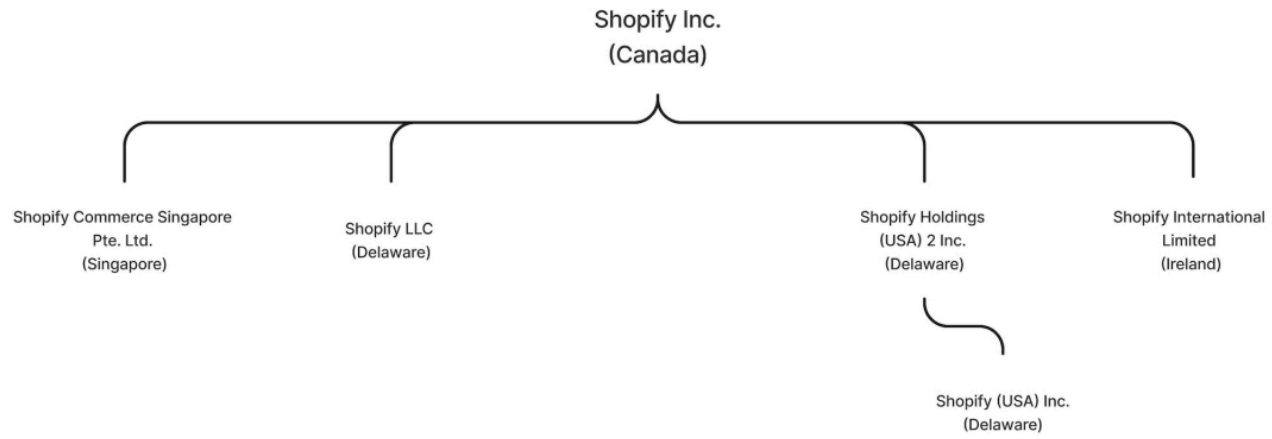
Where Shopify is engaged by a Merchant to conduct processing and both are responsible for harm caused by the processing in breach of this Processor Policy, Shopify accepts that both Shopify and the Merchant may be held liable for the entire damage in order to ensure effective compensation of the data subject.

Part V: Related policies and procedures

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: Processor 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 privacyoffice@shopify.com Reg no.: 303888502	Lithuania
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	Sweden

	privacyoffice@shopify.com Reg no.: 556838-0082	
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 privacyoffice@shopify.com Reg no.: 426160-7	Canada
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	USA

	privacyoffice@shopify.com Reg. no.: 6278610	
SC Commerce Services Inc.	Address: 251 Little Falls Drive, Wilmington, DE 19808 privacyoffice@shopify.com Corp. no.: 4756665	USA
Shopify Financial Services Inc.	Address: 251 Little Falls Drive, Wilmington, DE 19808 privacyoffice@shopify.com Corp. no.: 10042839	USA
Shopify Rebellion Inc.	Address: 251 Little Falls Drive, Wilmington, DE 19808 privacyoffice@shopify.com Corp. no.: 10066611	USA
Shopify Rebellion Brand Inc.	Address: 251 Little Falls Drive, Wilmington, DE 19808 privacyoffice@shopify.com Corp. no.: 10066614	USA
Shopify Search, Inc.	Address: 251 Little Falls Drive, Wilmington, DE 19808 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 privacyoffice@shopify.com Reg. no: 515098952	Israel
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.co	USA

[Appendix 2 – This Appendix 2 is intentionally blank in order to align the numbering of the appendices with the Controller Policy]

Appendix 3 - Data Protection Rights Procedure

1. Introduction

1.1 Data subjects whose personal data are processed by Shopify under the Processor Policy have certain data protection rights, which they may exercise by making a request to the controller of their information (i.e. a Merchant) (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 Processor 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.

(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.

(c) **The right to erasure:** This is the right for data subjects to obtain from a controller the erasure of personal data about them on certain grounds – for example, where the personal data is no longer necessary to fulfil the purposes for which it was collected.

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

(e) **The right to object:** This is the right for data subjects to object, on certain grounds, to a controller's processing of personal data about them.

(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 information to another controller, if certain grounds apply.

3. **Responsibility to assist the Merchant to respond to a Data Request**

3.1 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.

3.2 As such, when a data subject contacts Shopify to make any Data Request where Shopify processes that data subject's personal data as a processor on behalf of a Merchant under the Processor Policy, Shopify must inform the relevant Merchant promptly and provide it with reasonable assistance to help the data subject to exercise his or her rights in accordance with the Merchant's duties under applicable data protection laws.

4. Handling a Data Request

4.1 If a group member receives a Data Request from a data subject, it must pass the request 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 the Data Protection Team and other designated teams deal with the request.

4.2 The Data Protection Team and other designated teams will make an initial assessment of the Data Request as follows:

(a) they will determine 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 processor of the personal data on behalf of a Merchant, it shall pass the Data Request without undue delay and not later than 7 days after having become aware of it to the relevant Merchant and will help the Merchant fulfil the request in accordance with its contract terms with that Merchant and will not respond to the request directly unless required to do so by relevant law.

4.3 When Shopify must rectify or erase personal data on instruction of a Merchant when it is acting as a processor, Shopify will notify other group members and any sub-processor to whom the personal data has been disclosed so that they can also update their records accordingly.

5. Questions about this Data Protection Rights Procedure

5.1 All questions relating to this 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 Processor 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 and/or the appropriate highest level of management, where necessary. 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 BCRs.

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: Complaints 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** (Government Disclosure Request Policy) to the Processor 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 Processor 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 Processor 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 other 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 Processor 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 Processor 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 Processor 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 Processor Policy

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

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

4.2 Where relevant to a staff member's role, training will cover the following procedures under the Processor 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 all staff:

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

(b) have a working knowledge of the Processor 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 Processor Policy .

Appendix 6 - Audit Protocol

1. **Background**

1.1 Shopify must audit its compliance with the Processor 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 Processor 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 Processor Policy, this is only one way in which Shopify ensures that the provisions of the Processor 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 Processor 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 Processor 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 Processor 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 2.6 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 Processor

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

2.3 Where Shopify acts as a processor, the Merchant (or auditors acting on its behalf) may, pursuant to the terms of the Merchant's contract with Shopify, audit Shopify or its subprocessors for compliance with the commitments made in the Processor Policy. Where agreed by the Merchant, Shopify may fulfil such Merchant audit requirements by providing relevant and accurate evidence of recent data protection and information security audits to which they have been subject.

Frequency of audit

2.4 Audits of compliance with the Processor 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;

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

(d) as required by the terms of a Merchant's contract with Shopify.

Scope of audit

2.5 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;

(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 Processor 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

2.6 Audits of the Processor 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 Processor Policy (including any related procedures and controls).

2.7 If a Merchant exercises its right to audit Shopify for compliance with the Processor Policy, such audit may be undertaken by that Merchant or by an independent and suitably experienced auditor approved by that Merchant in accordance with the terms of the Merchant's contract with Shopify.

Reporting

2.8 After each audit, 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.

2.9 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 BCRs and the DPO will notify the lead supervisory authority in the annual update.

2.10 Upon request and subject to applicable law, Shopify will provide copies of the results of data protection audits of the Processor Policy (including any related procedures and controls):

(a) to the competent supervisory authorities; and

(b) subject to respect for the confidentiality and trade secrets of the information provided, to the extent that an audit of compliance with the Processor Policy relates to personal data Shopify processes on behalf of a Merchant, to that Merchant in accordance with Shopify's contract with the Merchant including in application of the confidentiality terms of such contract.

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

Supervisory authority audits

2.12 The competent supervisory authorities may audit group members for compliance with the Processor 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, in some circumstances.

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 Processor Policy.

1.2 This procedure will be made available to data subjects whose personal data is processed by Shopify under the Processor 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 Processor Policy or not) by e-mailing Shopify's Data Protection Team at privacyoffice@shopify.com or by writing to us at the address indicated in the Processor Policy under the heading 'How to raise questions or concerns'.

3. Complaints where Shopify is a Processor

3.1 *Communicating complaints to the Merchant*

3.1.1 Where a complaint is brought under the Processor Policy, Shopify will communicate the details of the complaint to the relevant Merchant by sending the entire complaint to the relevant Merchant without delay, in any event no later than 7 days from the receipt of the request. If the complaint mentions more than one Merchant, Shopify will redact the details of the other Merchants when sending the complaint to each Merchant.

3.1.2 If requested by the Merchant, Shopify will assist by providing the Merchant with reasonable information in its control relevant to the complaint in accordance with the terms of its contract with the Merchant.

3.2 *What happens if a Merchant no longer exists?*

3.2.1 Where a Merchant no longer exists or has become insolvent, and no successor entity has taken its place, data subjects whose personal data are processed under the Processor Policy have the right to complain to Shopify and Shopify will handle such

complaints, to the extent this is practical and possible, in accordance with the following procedure.

3.3 *Who handles complaints?*

3.3.1 The Data Protection Team will handle all such complaints. The Data Protection Team will work with colleagues from relevant product and service lines to address and resolve such questions, concerns and complaints.

3.4 *What is the response time?*

3.4.1 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.

3.4.2 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.

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

3.5.1 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).

3.5.2 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.

3.5.3 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.

3.5.4 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.

3.5.5 In such cases, data subjects also have the right to complain to a competent supervisory authority and to file a claim with a court of competent jurisdiction, including where they are not satisfied with the way in which their complaint has been resolved by Shopify. Such complaints and proceedings will be handled in accordance with paragraph 4 of this Complaint Handling Procedure.

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

4.1 Overview

4.1.1 Where a data subject is conferred third party beneficiary rights under Part IV of the Processor 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 4.12(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 Processor 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 Processor 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 Processor 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 Processor 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 Processors.

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

2.4 Shopify agrees that:

(a) a supervisory authority may audit the compliance with the Processor Policy of any group member for which it is competent; and

(b) a competent supervisory authority may audit any group member who processes personal data for a Merchant established within the jurisdiction of that supervisory authority for compliance with the Processor Policy, in accordance with the applicable data protection law(s) of its jurisdiction.

2.5 Shopify agrees to abide by a formal decision of any competent supervisory authority on any issues relating to the interpretation and application of the Processor Policy (unless and to the extent that Shopify is entitled to appeal any such decision and has chosen to exercise such right of appeal).

2.6 Shopify agrees that any dispute related to the competent supervisory authority's exercise of supervision of compliance with the BCRs will be resolved by the courts of the European jurisdiction of that supervisory authority, in accordance with that European jurisdiction’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 Processor Policy to its Merchants, to Shopify group members bound by the Processor 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 Processor 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 Processor Policy. Shopify must provide this information upon request to competent supervisory authorities, and to Merchants who benefit from the Processor Policy.

2.3 Shopify must also maintain an accurate and up-to-date list of the subprocessors appointed by Shopify to process personal data on behalf of Merchants, where Shopify is acting as a processor. Shopify must provide this information upon request to competent supervisory authorities, and to Merchants who benefit from the Processor Policy.

2.4 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 Processor Policy

3.1 The Data Protection Team will review and, where necessary, update Shopify's Processor Policy on a regular basis and in response to any relevant new developments, (for example changes to the scope of the BCR-P, 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 Processor Policy.

No changes to the Processor Policy shall take effect unless reviewed and approved by the Data Protection Team.

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

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

(b) to Merchants who benefit from the Processor Policy via the Shopify corporate website at https://www.shopify.com (and, if any changes are material in nature, Shopify must also actively communicate the material changes to Merchants before they take effect, in accordance with paragraph 4.2 below); 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 Processor Policy.

4. Communication of material changes

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

4.2 If a proposed change to the Processor Policy will materially affect Shopify's processing of personal data as a processor on behalf of a Merchant, Shopify will also:

(a) actively communicate the proposed change to the affected Merchant before it takes effect, and with sufficient notice to enable the affected Merchant to raise objections; and

(b) the Merchant may then suspend the transfer of personal data to Shopify and/or terminate the contract, in accordance with the terms of its contract with Shopify.

5. **Transfers to new group members**

5.1 If Shopify intends to transfer personal data to any new group members under the Processor Policy, it must first ensure that all such new group members are bound by the Processor 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 BCR-P in accordance with the laws of the country of destination. This Appendix relates to **Rule 9** and **commitment 10** of Part III of the BCRs.

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 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.

2.3 Even where disclosure is required, if the request concerns personal data for which the Merchant is the controller, then Shopify's policy is that the Merchant should have the opportunity to protect the personal data requested. This is because the Merchant, as controller, has the greatest interest in ensuring the lawfulness of, and is in a better position to comply with, the Disclosure Request.

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 BCRs 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 Merchant.

3.1.2 Such notification regarding a Disclosure Request under paragraph 3.1.1 should include, where available: details of the personal data requested, the requesting body, the legal basis for 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 BCRs 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 suspend the effects of the Disclosure Request until the matter has been resolved. 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 9** of Part III of the BCRs (i.e. the obligation to notify the DPO if it has reason to believe that it cannot comply with the BCRs).

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.

3.2.3 If Shopify's Data Protection Team determines that disclosure is required pursuant to paragraph 2, Shopify's Data Protection Team will further review on a case-by-case basis whether and how to notify the Merchant and/or competent supervisory authorities in accordance with paragraph 4.

4. Notice of a Disclosure Request

4.1 Notice to the Merchant

4.1.1 If a request concerns personal data for which a Merchant is the controller, Shopify will ordinarily ask the Requesting Authority to make the Disclosure Request directly to the relevant Merchant, and Shopify will support the Merchant in accordance with the terms of its contract to respond to the Disclosure Request. This is because the Merchant, as controller, has primary legal responsibility and control over the data at issue. For that reason, unless it is legally prohibited from doing so or there is an imminent risk of serious harm, Shopify will advise the Requesting Authority to address the Disclosure Request to the Merchant.

4.1.2 If this is not possible (for example, because the Requesting Authority declines to make the Disclosure Request directly to the Merchant), Shopify will notify and provide the Merchant with the details of the Disclosure Request prior to disclosing any personal data, unless legally prohibited or where an imminent risk of serious harm exists that prohibits prior notification.

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.

4.2.2 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

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

2. Transfer Risk Assessment

This Appendix relates to **Rule 12** and **commitment 9** of Part III of the Processor Policy and sets out the elements that should be considered when undertaking a transfer risk assessment:

2.1 the specific circumstances of the transfer, including:

(a) the type of recipients;

(b) economic sector in with 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.

2.2 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

2.3 any safeguards in addition to those under the BCRs, 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 Processor Policy

1. Background

1.1 Shopify's Processor 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 Processor 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.

2. Data processed on behalf of merchants

Who transfers the personal data described in this section?	Every Shopify group member inside of Europe may transfer the personal data that they process on behalf of a third-party controller 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 process on behalf of a third-party controller described in this section to every Shopify group member inside and outside of Europe. Transfers made directly from a third-party controller (whether inside or outside of Europe) directly to a group member as processor (whether inside or outside of Europe) will also be within the scope of the Processor Policy.
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 or third-party controllers 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 or third-party controllers inside and outside of Europe.
What categories of personal data are transferred?	All personal data that Shopify processes as a processor on behalf of its merchants. For example, Shopify is a processor of merchant customer personal data comprised within transactions placed by customers with merchants using Shopify's platform. The personal data transferred will comprise any personal data that a controller chooses to upload to Shopify's platforms for processing. Shopify does not determine or control the personal data that third-party controllers may choose to upload to its platform.
What special categories of personal data (if any) are transferred?	The order information that Shopify processes on behalf of merchants will include details of purchased products (which may be wide-ranging). However, Shopify group members do not intentionally collect or process any special categories of personal data on behalf of controllers.
Who are the types of data subjects whose personal data are transferred?	This will comprise any data subjects whose personal data a controller chooses to upload to Shopify's platform(s) for processing. Shopify does not determine or control the data subjects about whom third-party controllers may choose to upload personal data to its platform(s).

Why is this personal data transferred and how will it be used?	Personal data processed on behalf of merchants is transferred for the purposes of providing Shopify's products and services.
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**.