Afterpay - Cross Border Privacy Terms

LAST UPDATED: 13 March 2023

These Cross Border Privacy Terms apply and form part of the global Master Services Agreement and applicable regional statement of work ("**SOW**") or other regional written or electronic merchant agreement ("**Merchant Agreement**") for the provision of deferred payment services by Afterpay to Merchants (the SOW and/or the Merchant Agreement (as applicable) are each referred to as the "**Afterpay Agreement"**) to reflect the parties' agreement with regard to the processing of personal information. Any references to 'personal data' shall be construed with the same meaning as 'personal information'.

In these Cross Border Privacy Terms:

- Afterpay means the Afterpay legal entity identified in the SOW or Merchant Agreement; and
- Merchant means the merchant legal entity identified in the SOW or Merchant Agreement

By entering into the Afterpay Agreement, Merchant enters into these Cross Border Privacy Terms. Any capitalised terms not otherwise defined in these Cross Border Privacy Terms have the same meaning as set out in the Afterpay Agreement.

Subject to Afterpay providing Merchant written notice of approved Territories where Merchant may allow Cross Border Transactions, the following terms shall apply when processing personal data in relation to such Cross Border Transactions in the approved Territories. For the avoidance of doubt, not all Territories are currently available to Merchants for Cross Border Transactions.

Territory	**Terms**
Cross Border Transactions for Customers in Australia	You and we will, when performing obligations in relation to Cross Border Transactions for Customers located in Australia, comply with any applicable laws and regulations relating to the collection or handling of personal information in Australia, including the Privacy Act 1988 (Cth).
Cross Border Transactions for Customers in New Zealand	You and we will, when performing obligations in relation to Cross Border Transactions for Customers located in New Zealand, comply with any applicable laws and regulations relating to the collection or handling of personal information in New Zealand, including the Privacy Act 2020.
Cross Border Transactions for Customers in Canada	You and we will, when performing obligations in relation to Cross Border Transactions for Customers located in Canada, comply with any applicable laws and regulations relating to the collection or handling of personal information in Canada, including The Personal Information Protection and Electronic Documents Act (PIPEDA), Personal Information Protection Act (British Columbia), Personal Information Protection Act (Alberta),Personal Information Protection Act (Quebec), and Bill 64, the Act to modernize legislative provisions as regards the protection of personal information (Quebec).
Cross Border Transactions for Customers in the USA	You and we will, when performing obligations in relation to Cross Border Transactions for Customers located in the USA, comply with any applicable laws and regulations relating to the collection or handling of personal information in the USA, including the Gramm-Leach-Bliley Act, the California Financial Information Privacy Act (CalFIPA) the California Consumer Privacy Act of 2018 (CCPA), the California Privacy Rights Act of 2020 (CPRA), the Virginia Consumer Data Protection Act (VCDPA), the Colorado Privacy Act (CPA), the Personal Data Privacy and Online Monitoring Act in Connecticut (CTDPA),

	and the Utah Consumer Privacy Act (UCPA).
Cross Border Transactions for Customers in the United Kingdom	You and we will, when performing obligations in relation to Cross Border Transactions for Customers located in the United Kingdom, each comply with the Data Sharing Terms set out below.
Cross Border Transactions for Customers in the European Economic Area	You and we will when performing obligations in relation to Cross Border Transactions for Customers located in the European Economic Area, each comply with the Data Sharing Terms set out below.

Data Sharing Terms

1. **Interpretation**

1.1. Where there is a reference to “United Kingdom” or “UK” and “UK GDPR” in these Data Sharing Terms, a party shall interpret the obligations and rights to also refer to the “European Economic Area” and “GDPR” respectively if applicable to the processing of Shared Personal Data under these Data Sharing Terms.

1.2. In the event of any conflict between the provisions of these Data Sharing Terms and any provision of the Afterpay Agreement, these Data Sharing Terms shall prevail to the extent of inconsistency.

2. **Obligations of the parties**

2.1. The parties acknowledge and agree that in relation to the Shared Personal Data, each party acts as a Data Controller in its own right. Each party acknowledges that one party ("**Data Discloser**") will regularly disclose to the other party ("**Data Receiver**") the Shared Personal Data for the Permitted Purposes.

2.2. Each party shall comply with its obligations under the Data Protection Laws at all times during the Term of the Afterpay Agreement. In particular, each party shall:

(a) nominate a single point of contact ("**POC**") for the purposes of these Data Sharing Terms (as identified in Appendix 2 to these Data Sharing Terms or as otherwise notified to the other party from time to time in writing);

(b) ensure that the Shared Personal Data is not irrelevant or excessive with regard to the Permitted Purposes;

(c) ensure that it processes the Shared Personal Data fairly and lawfully during the term of the Afterpay Agreement;

(d) inform the Data Subjects, on or before the date when that party commences the processing of their Personal Data, of the purposes for which it will process their Personal Data and to provide all the information that it is obliged to provide under Data Protection Laws to ensure that the Data Subjects understand how their Personal Data will be processed by that party; and

(e) be responsible for dealing with its own requests from Data Subjects under Data Protection Laws in relation to the Shared Personal Data and shall provide such assistance as is reasonably required to enable the other party to comply with such requests.

2.3. The Data Receiver shall not retain or process Shared Personal Data for longer than is necessary to carry out the Permitted Purposes and shall be responsible for implementing appropriate measures to ensure the Shared Personal Data is destroyed or deleted at the end of such periods.

2.4. Notwithstanding paragraph 2.3, each party may continue to retain Shared Personal Data in accordance with any applicable statutory or professional retention periods.

2.5. The Data Receiver may only transfer Shared Personal Data to a third party located outside the EEA provided that it ensures that: (i) the transfer is to a country approved by the European Commission as providing adequate protection pursuant to Article 45 GDPR; (ii) there are appropriate safeguards in place pursuant to Article 46 GDPR; or (iii) one of the derogations for specific situations in Article 49 GDPR applies.

2.6. Where Afterpay transfers Shared Personal Data to Merchant at a location outside the EEA in circumstances where such transfer is not subject to any of the permitted derogations or conditions contained in the GDPR such that in the absence of the protection for the transferred Shared Personal Data provided pursuant to these Data Sharing Terms, the relevant transfer would be prohibited by the GDPR, Afterpay (as "data exporter") and Merchant (as "data importer") enter into and agreed to be bound by the Standard Contractual Clauses.

2.7. The Data Receiver may only transfer Shared Personal Data to a third party located outside of the United Kingdom provided that it ensures that: (i) the transfer is to a country approved by the United Kingdom as providing adequate protection pursuant to Article 45 of UK GDPR; (ii) there are appropriate safeguards in place pursuant to Article 46 of UK GDPR; or (iii) one of the derogations for specific situations in Article 49 of UK GDPR applies to the transfer.

2.8. Where Afterpay transfers Shared Personal Data to Merchant at a location outside the United Kingdom in circumstances where such transfer is not subject to any of the permitted derogations or conditions contained in UK Data Protection Law such that in the absence of the protection for the transferred Shared Personal Data provided pursuant to these Data Sharing Terms, the relevant transfer would be prohibited by UK Data Protection Law, Afterpay (as "data exporter") and Merchant (as "data importer") enter into, and agree to be bound by, the Standard Contractual Clauses.

2.9. In the event that the Standard Contractual Clauses are amended, replaced and/or superseded from time to time, Merchant and Afterpay shall enter into such amended, replaced and/or superseded standard contractual clauses approved by a competent authority.

2.10. Each party shall implement and maintain appropriate technical and organisational measures to ensure a level of security appropriate to the risk (taking into account the nature, scope, context and Permitted Purposes of processing the Shared Personal Data), including from unauthorised or unlawful processing of such Shared Personal Data, or accidental loss or destruction of, or damage to, such Shared Personal Data.

2.11. The parties shall each comply with its obligation to report a Personal Data Breach relating to the Shared Personal Data to the applicable supervisory authority and (where applicable) Data Subjects under Articles 33 and 34 of UK GDPR and shall each inform the other party of any Personal Data Breach without undue delay (and in any event, within 48 hours of becoming aware) irrespective of whether there is a requirement to notify any supervisory authority or Data Subjects. Without limiting the foregoing, the parties agree to provide reasonable assistance as is necessary to each other to facilitate the handling of any Personal Data Breach relating to the Shared Personal Data in an expeditious and compliant manner.

2.12. In the event of a dispute or claim brought by a Data Subject or a supervisory authority concerning the processing of Shared Personal Data against either or both of the parties, the parties shall inform each other about any such disputes or claims and will cooperate with a view to settling them amicably in a timely fashion.

3. **Data Secrecy**

3.1. The parties shall take reasonable steps to ensure the reliability of any employee, agent or contractor who may have access to the Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know and/or access the Shared Personal Data, as strictly necessary for the purposes of the Afterpay Agreement, and to comply with any applicable laws in the context of that individual's duties to the parties, ensuring that all such individuals are subject to confidentiality

undertakings or professional or statutory obligations of confidentiality.

3.2. Each party shall be obliged to ensure that persons authorized to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality relating to the Personal Data and processing activities covered by the Afterpay Agreement and these Data Sharing Terms.

4. **Data Processors**

4.1. Where the Data Receiver appoints a Data Processor to process the Shared Personal Data, it shall comply with Article 28 of the UK GDPR and shall remain liable to the Data Discloser for the acts and/or omissions of the Data Processor.

4.2. Data Receiver shall choose such Data Processor diligently with special attention to its good standing and experience.

4.3. Data Receiver shall enter into a written contract with any Data Processor and such contract shall impose upon the Data Processor the same obligations as imposed by the UK GDPR.

5. **Indemnity**

5.1. Each party ("**Indemnifying Party**") undertakes to indemnify the other party ("**Indemnified Party**") from all claims, liabilities, costs, expenses, damages, fines and losses the Indemnifying Party causes the Indemnified Party as a result of the Indemnifying Party's breach of any of the provisions of these Data Sharing Terms.

6. **Definitions**

6.1. In these Data Sharing Terms:

(a) **Clarifications** means the following clarifications in respect of the EU SCCs agreed by Afterpay (as "data exporter") and Merchant (as "data importer"): (a) Clause 7 (Docking clause) shall not apply; (b) the optional wording in Clause 11 (Redress) relating to an independent dispute resolution body shall not apply; (c) Annex IA shall be populated with details of the Parties set out in Data Sharing Terms and the Afterpay Agreement; (d) Annex IB shall be populated by the description of processing of personal data set out set out in Appendix 2 and (e) Annex II shall be populated with the technical and organisational security measures detailed in Appendix 3.

(b) **Data Controller** has the meaning given to it in the Data Protection Laws (as applicable);

(c) **Data Processor** has the meaning given to it in the Data Protection Laws (as applicable);

(d) **Data Protection Laws** means any applicable laws and regulations in any relevant jurisdiction relating to the use or processing of personal data including without limitation: (i) in the UK, the UK Data Protection Law and (ii) in the European Economic Area (the "**EEA**"), the General Data Protection Regulation EU 2016/679 ("**GDPR**") and any laws and regulations implementing or made pursuant to EU Directive 2002/58/EC (as amended by 2009/136/EC); in each case, as updated, amended or replaced from time to time.

(e) **Data Subject** means a potential Customer or a Customer who is the subject of Personal Data and as set out in Appendix 2 to the Data Sharing Terms;

(f) **EU SCCS** means Module One of the standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 (the "GDPR") issued by the European Commission in the Commission Implementing Decision (EU) 2021/914 of 4 June 202 (the full text of which is available at https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc/standard-contractual-clauses-international-transfers_en)

as amended or replaced from time to time by a competent authority under applicable data protection laws.

(g) **Personal Data** has the meaning given to it in the Data Protection Laws (as applicable);

(h) **Personal Data Breach** has the meaning given to it in the Data Protection Laws (as applicable);

(i) **Permitted Purpose** is as detailed in Appendix 2 to these Data Sharing Terms;

(j) **Shared Personal Data** means the Personal Data to be shared between the parties under the Afterpay Agreement as set out in these Data Sharing Terms;

(k) **Standard Contractual Clauses** means the EU SCCs as amended by the UK Addendum and incorporated into these Data Sharing Terms (and the Afterpay Agreement) by reference and subject to the additional information and clarifications set out in Appendix 1 to these Data Sharing Terms;

(l) **UK Addendum** means the international data transfer addendum to the European Commission's standard contractual clauses for international data transfers as approved by the UK Parliament and published by the UK Information Commissioner's Office (the full text of which is available at https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf);

(m) **UK Data Protection Law** means the UK Data Protection Act and the UK GDPR.

(n) **UK GDPR** shall have the meaning given to this term in section 3 of the UK Data Protection Act.

APPENDIX 1

UK Addendum to the EU SCCs

The tables in Part 1 of the UK Addendum are populated as follows:

Table 1: Parties

Start date	The date of the Afterpay Agreement.	
The Parties	**Exporter (who sends the Restricted Transfer): Afterpay**	**Importer (who receives the Restricted Transfer): Merchant**
Parties' details	Please see the main body of the Afterpay Agreement for the details of the Parties.	
Key Contact	The appropriate point of contact for Afterpay is privacy_counsel@squareup.com. The appropriate point of contact for the Importer is set forth in the Afterpay Agreement or has been otherwise communicated in writing by Merchant to Afterpay.	

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	This Addendum is appended to the EU SCCs as applicable and as incorporated by reference into this Appendix (and the Afterpay Agreement) with additional details required by the EU SCCs as set out in the Clarifications (as the EU SCCs may be amended or replaced from time to time by a competent authority under applicable data protection laws)**.**

Table 3: Appendix Information

"Appendix Information" means the information referenced at (d) and (e) of the definition of "Clarifications" in these Data Sharing Terms.

Annex 1A: List of Parties: The Parties are Afterpay and Merchant, as each is defined in the Afterpay Agreement.
Annex 1B: Description of Transfer: Please see the information referenced at (d) of the definition of "Clarifications" in these Data Sharing Terms.
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: Please see the information referenced at (e) of the definition of "Clarifications" in these Data Sharing Terms.
Annex III: List of Sub processors (Modules 2 and 3 only): Not required

Table 4: Ending this Addendum when Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	**Which Parties may end this Addendum as set out in Section 19 of the UK Addendum:** **☐ Importer** **☒ Exporter** **☐ neither Party**

APPENDIX 2

A. LIST OF PARTIES

Data exporter(s): Afterpay (We, Our)
Data importer(s): Merchant (You, Your) (see the Afterpay Agreement for the contact details of the Data exporter and the Data importer)

B. DESCRIPTION OF TRANSFER

The personal data transferred between the parties, including the categories thereof and the purposes intended, are as described in **Tables 1(a)** and **(b)** below.

Sensitive data transferred
It is not intended for any sensitive data to be transferred between the parties.

The frequency of the transfer
Data is transferred on a continuous basis as necessary to support the provision and receipt of Services as between Afterpay and the Merchant.

Nature of the processing
The personal data transferred will be subject to processing which shall have the meaning given to the term in the UK GDPR as updated, amended and replaced from time to time and any associated or national implementing legislation regarding data protection.

Purpose(s) of the data transfer and further processing
Provision of the Services by Afterpay to Merchant pursuant to the Afterpay Agreement and such other instructions as may be provided by either party from time to time.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period
The period set out in the relevant Data Retention policies of the data exporter or as otherwise required by applicable legal obligations.

For transfers to (sub-)processors, also specify subject matter, nature and duration of the processing
The subject matter and the nature of such processing will be as specified above under the headings "Categories of personal data transferred" and "Nature of the processing" respectively. The duration of such processing will be no longer than is reasonably necessary for the purposes of such processing.

C. COMPETENT SUPERVISORY AUTHORITY

The competent supervisory authority shall be the Information Commissioner's Office, the UK supervisory authority.

Table 1 (a)

Shared Personal Data provided by You to Afterpay (including Data Subject)	**Permitted Purpose**
● First name, surname and mobile number of potential Customers and Customers ● Email address and IP address of potential Customers and Customers	For the purpose of enabling Afterpay to: ● undertake fraud prevention; and, ● on-board the Customer

• Customer address • Customer order number • Customer first name, surname and email address	For the purpose of enabling Afterpay to deal with Customer complaints relating to the service We provide to Customers
First name, surname, email address and contact number of Your employees	For the purpose of Afterpay performing Our obligations under the Afterpay Agreement

Table 1 (b)

Shared Personal Data provided by Afterpay to You (including Data Subject)	**Permitted Purpose**
• Customer address • Customer order number • Customer first name, surname and email address	For the purpose of enabling You to: • deliver Goods to Customers where Merchant utilises the Afterpay express checkout function on their Website; • deal with Customer complaints relating to the services You provide to Customers; • deal with refunds and/or orders and queries from Customers in relation to refunds and/or orders (via the Merchant Portal or otherwise)
First name, surname, email address and contact number of Afterpay employees	For the purpose of You performing your obligations under the Afterpay Agreement

Contact points for data protection enquiries:

Data Exporter: privacy_counsel@squareup.com

Data Importer: As otherwise communicated in writing by Merchant to Afterpay.

APPENDIX 3

TECHNICAL AND ORGANISATIONAL MEASURES

1. **FRAMEWORK:** The data importer has put in place a variety of technical and organisational security measures to protect Personal Data.
2. **POLICIES:** The data importer is subject to data security requirements set forth in its policies, procedures, standards and guidelines that define various aspects of required protection for personal data.
3. **STAFF EDUCATION, TRAINING AND RESPONSIBILITIES:** The data importer provides continuous data privacy and information security education for all relevant employees upon hire.
4. **INCIDENT MANAGEMENT:** The data importer maintains documented policies and procedures to respond to, and document responses to, relevant disruptions and events. The data importer performs testing of these procedures and provides education to relevant staff at least annually.
5. **USER ACCESS TO INFORMATION SYSTEMS:** The data importer maintains password-based, badge-based, and/or multi-factor authentication mechanisms. The data importer employs role-based access controls and grants the least privilege necessary for job function.
6. **PHYSICAL ACCESS CONTROL:** The data importer maintains badge-based and role-based physical access controls for all offices and data center locations that house sensitive information. The data importer maintains role-based access controls and full-disk encryption on portable IT assets such as laptops.
7. **IT SYSTEM SECURITY:** It is the data importer's policy that business units implement various controls, processes and standards for safeguarding IT systems
8. **DATA LEAKAGE/MEDIA HANDLING/CRYPTOGRAPHIC CONTROLS:** The data importer employs data encryption, role-based access controls, network segmentation via firewalls, log/event monitoring, and automated 24/7 incident alerting to minimize the risk of data leakage.
9. **THIRD PARTY SERVICE PROVIDERS:** The data importer vets all third party service providers to ensure that the processing of data by such providers meets the data importer's Merchant security guidelines. Third party service providers are subject to agreements governing the handling and processing of personal data on behalf of the data importer.
10. **STORAGE OF PERSONAL DATA:** Personal Data is to be kept only for as long as is necessary in accordance with the data importer's Data Policy and relevant local laws and regulations.
11. **DISPOSAL OF PERSONAL DATA:** When Personal Data is no longer required for business, legal or regulatory obligations, the data importer securely destroys the data.