Global Online GDPR Centre

Revised 24 February 2023

Welcome to the Airwallex Global Online GDPR Centre

Airwallex is committed to protecting the privacy of everyone who engages with our platform. We also value the importance of transparency with respect to our privacy practices.

We created this Airwallex Privacy Center to help you find answers to frequently asked questions about how we collect and use personal data, the rights that individuals have in relation to personal data held by Airwallex, and how Airwallex complies with international data protection laws, such as the General Data Protection Regulation (**GDPR**) of the UK and EU.

This content is not legal advice, has been published for your general information purposes only, may not be exhaustive or current and may be amended from time to time without notice to you.

What is the GDPR?

The GDPR is the data protection regulation that gives individuals more control over their personal data. The European Union (**EU**) and United Kingdom (**UK**) have separate but similar versions of the GDPR.

Under the GDPR, organisations must take great care when processing personal data. Organisations must ensure there is a legal basis for every data processing activity and they must tell people how and why data is used. Individuals also have greater rights under the GDPR, and organisations must be accountable for all processing.

In addition, certain requirements must be satisfied before EU / UK individuals' personal data may be transferred outside the EU or the UK, unless the organisation receiving the personal data is located in a permitted jurisdiction white listed by the European Commission or UK government. The list of white listed permitted jurisdictions may be found on the European Commission's website **here** or the UK government website **here**.

What is personal data?

Personal data is any information that is related to an identified or identifiable natural person (e.g. you), such as your name, email address, username, ID, bank account number, card details, telephone number, personnel number, number plate, appearance, customer number or address. The definition under the GDPR is broad, and can include information that could be used indirectly and/or with other information to identify a natural person – such as device identifiers or IP address.

What does 'processing' mean in this context?

Processing means any operation that is performed on personal data, 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.

Who does the GDPR apply to?

The GDPR applies to any data processor or data controller in the EU or UK that processes personal data, as well as any data processor or data controller outside the EU or UK that processes the personal data of individuals in the EU or UK residents where the processing activities are related to:

1. offering goods or services to data subjects in the EU or UK (even if those goods or services are provided free of charge); or
2. monitoring the behaviour of individuals taking place in the EU or the UK.

Global Privacy Policy

You can learn about how we collect, use and share information in our Global Privacy Policy. Our Global Privacy Policy can be found at this link.

Is Airwallex acting as a data controller or a data processor?

Airwallex is an independent data controller of the data it processes.. Such data processing activities include (among other things):

1. providing the Airwallex products and services;
2. developing new, or enhancing existing, products;
3. providing customer support;
4. monitoring, detecting and preventing fraudulent activities on our platform; and
5. complying with the legal and regulatory obligations that apply to Airwallex.

A "data controller" is the entity that determines the purposes and means of the data processing taking place, i.e. the main decision maker that exercises overall control over the data processing. For example, a data controller would make decisions on what types of personal data to collect and for what purpose(s).

A "data processor" is an entity that acts on behalf of and at the direction of a data controller in processing personal data. As the data processor is acting on the instructions of the data controller, it does not exercise control or decision making over the processing of personal data.
Data controllers and data processors have different responsibilities under the GDPR – for example, controllers are in charge of identifying a lawful purpose or legal basis, and must facilitate individual rights requests.

The specific Airwallex entity that acts as data controller in respect of your personal information depends on your country of residence and the entity which you used to enter into an agreement with Airwallex to provide services to you. You can read more about which Airwallex entity is your data controller in Section 2 of our Global Privacy Policy.

Do customers act as data controllers or data processors?

Business customers generally act as independent data controllers because it is up to the business customer to decide what personal data (e.g. personal data of their end user, end customer, beneficiary or payee) they collect for their own business purposes. This processing purpose is separate from business purposes for which personal data is collected or received by Airwallex even if the personal data involved is the same data.

However, in some cases, business customers can also act as data processors on our behalf, such as when, in connection with the Airwallex for Platform product, business customers facilitate the collection of certain personal data of their customer that is required by Airwallex for KYC and onboarding purposes.

What 'lawful purpose' or 'legal basis' does Airwallex rely on to process personal data?

Airwallex relies upon a number of legal grounds to process personal data.

Please refer to Section 4 of our Global Privacy Policy for an overview of the types of personal data we collect from you, and the applicable 'legal basis' for each.

What rights do I have over my data?

Depending on your location, you may have certain rights to your personal data. If Airwallex is a data controller of your personal data then we are responsible for managing and responding to your request.

You can read more about your rights and how you can exercise your rights in Section 7 of our **Global Privacy Policy**.

Who does Airwallex transfer data to? Are they all processors and sub-processors, and how are they evaluated?

In order for us to provide the Airwallex products and services, we will need to transfer personal data to different affiliates within the Airwallex Group and various external third parties.

Whether the Airwallex affiliates or external third parties are independent data controllers or data processors will depend on the nature of the data processing.

In general, the recipient is an independent data controller where it is processing personal data as part of its role to initiate or otherwise enable payments, transfers or financial transactions to occur, or where the recipient is an Airwallex partner that also provides services independently to Airwallex's customers. For example, Airwallex will transfer data to our banking partners to facilitate transfers or collections, or at the request of customers, allow ecosystem partners who provide accounting services to customers to receive such customers' data. The recipient could also be a third party service provider, who act as a data processor to provide services to Airwallex. Regardless of whether the recipient is a data controller or data processor, we make sure we have appropriate safeguards in place to protect any personal data that is processed, including where relevant, through contractual obligations.

in respect of third party service providers who are data processors or sub-processors Airwallex vets and evaluates such third party service providers through our vendor management program prior to engaging them. As required under the GDPR, the contract with each data processor will also have the required GDPR safeguards to regulate the transfer to, and processing of data by the data processor or sub-processor. All potential vendors are also vetted and approved through Airwallex's information security review process before we use their services. This means we investigate their security standards, check their certifications, etc. and ensure they are able to adequately protect and ensure the security of personal data, before we consider sharing any data.

Types of Third Party Recipients	Purpose
Third party service providers	We engage a variety of service providers (who act as data processors) to enable us to provide our Services to you. For example, service providers may be used to: facilitate payment processing, support technology or infrastructure, cloud storage, conduct market research, marketing analytics, detect fraud, verify identity and perform audits or other functions. We will share your personal information with such service providers only to the extent necessary to allow the performance of their intended engagement. All service providers that receive your personal information are contractually bound to protect and use your information only in accordance with terms of the relevant contract.

Our corporate affiliates	To facilitate or support us in providing products and services to you or in order to provide services to each.All Airwallex group companies may only use your personal information in accordance with the relevant Intra-Group contracts governing such processing.
Ecosystem and Banking Partners	Our Services may be offered to you in conjunction with or facilitated by other financial institutions or other ecosystem partners (such as provider of accounting or treasury management services).Such Partners may have access to your personal information but only to the extent required to enable use by you of our or their products and services or otherwise as authorised or requested by you.
Regulatory Authorities: regulators, judicial authorities and law enforcement agencies, and other relevant third parties	There are circumstances in which we are legally required to disclose information about you to authorities, such as to comply with a legal obligation or processes, enforce our terms, protect our business and systems, address issues relating to security or fraud, or protect our users. These disclosures may be made with or without your consent, and with or without notice, in compliance with the terms of valid legal process such as a subpoena, court order, or search warrant. We are usually prohibited from notifying you of any such disclosures by the terms of the legal process. We may also disclose your information to: ● enforce our customer agreements, the Acceptable Use Terms or other applicable agreements or policies, including investigation of any potential violation thereof; ● detect, prevent or otherwise address security, fraud or technical issues; ● protect the integrity of our products and services, our rights, property, privacy, or security, or that of others, as permitted by law; or ● comply with applicable law, legal process or governmental orders.
Social Media Platforms	Social media networks such as Facebook, Twitter, Pinterest, and Instagram that offer functionalities, plugins, widgets, or tools in connection with our website or mobile application (e.g., to log into an account, or to share content with your friends and followers on social media). If you choose to use these functionalities, plugins, widgets, or tools, certain information may be shared with or collected by those social media companies—for more information about what information is shared or collected, and how it is used, see the applicable social media company's privacy policy.

Potential Acquirers of our business	If we are the subject or are involved in any corporate merger, acquisition, consolidation, reorganisation, sale, joint venture, assignment, transfer or other disposition of all or any portion of our business, assets or stock (including in connection with bankruptcy or similar proceedings), we may share data with third parties during negotiations. In the event your personal information becomes subject to a different privacy policy, we will make reasonable efforts to notify you beforehand. We also may need to disclose information to a third party in connection with a commercial transaction where we or any of our affiliates are seeking financing, investment or funding.
Other Authorised Parties	If you request (as part of the Service provided to you) or provide your consent, we may share your information including your personal information with a third party not defined in this Policy. Such third parties may include third party financial service providers, including but not limited to account information service providers and payment initiation service providers. Such disclosure will only be carried out in the manner you requested or consented to, and/or the manner described to you (whether by us or the relevant third party) at the time you agreed to the sharing, and in accordance with applicable law. Authorising a third-party service provider, application or website to access your Airwallex account or participating in certain promotional activities constitutes such request and consent to share your information.

For your reference, we have listed below Airwallex's typical third party processors and sub-processors:

Vendor	**Data**	**Purpose of processing**	**Country of primary contracting entity**
i2c	User data and user's customers' data	Transaction processing, card issuing and maintenance	United States
Google Cloud Platform	User data and user's customers' data	Cloud service provider	United States
Alibaba Cloud Platform	User data and user's customers' data	Cloud service provider	Hong Kong
Zendesk	User data and information provided to Airwallex support by users	Customer support services	United States
Trulioo Information Services	User data and User's customers' data	User identity verification and fraud detection	Canada
Refinitiv	User data and User's	User identity verification	United Kingdom

	customers' data	and fraud detection	
Visa	User data and User's customers' data	Transaction processing, card issuing, and maintenance	United States
Mastercard	User data and User's customers' data	Card payment acquiring	United States
Megaport	Encrypted data shared between cloud providers	Network connectivity between cloud providers	United States
Cloudflare	User data and User's customers data	Network security and anti-DDoS	United States
Valitor	User data and User's customers data	Card payment acquiring	Iceland
Splunk	Airwallex platform analytics and User data	Platform analytics, outage detection, and security monitoring	United States
Google	Limited User data and internal data	Document creation and processing, mail provider	United States
Zoom Video Communications	User data, insofar as that is shared in spoken word between the conversing parties, or recorded on the system	Video conferencing system	United States
Idemia	Cardholder name, PAN, CVV, expiration date, shipping address	Printing the cards for issuing	United States / Australia
Concentrix	Customer data	Customer service support function	Philippines
Salesforce	User data	Customer relationship management platform which stores User contact information as well as supporting information about the business relationship	United States
New Relic	Airwallex platform analytics	Platform analytics and outage detection	United States
Sumologic	Airwallex platform analytics	Platform analytics and outage detection	United States
Equinix	User data	Hardware data centre	United States

		services	
Hubspot	User data	Customer relationship management	United States
Mailgun	User data and User's customers data	Email notification services	United States
SendGrid	User data and User's customers data	Email notification services	United States
SendCloud	User data and User's customers data	Email notification services	China

What is a Data Processing Agreement and how can I get one with Airwallex?

A Data Processing Agreement (**DPA**) is a contract that under GDPR is mandated between a data controller and a data processor, which sets out the roles and responsibilities of the parties when personal data is processed, but not between data controllers. For our customers, our standard contract contains relevant data processing terms governing your relationship with Airwallex, who acts as an independent data controller.

International data transfers

The information presented below is for general information purposes only and is not legal advice. As rules surrounding international data transfers may vary across jurisdictions, please consult with your own legal counsel to familiarise yourselves with the requirements that govern your specific situations. For more information on where your information may be transferred, please refer to Section 5 of our Global Privacy Policy.

How does Airwallex deal with international data transfers?

Airwallex uses a set of Standard Contractual Clauses (SCCs) published by the European Commission for cross-border data transfers (in the form of a legal contract) to provide a legal mechanism to transfer EEA or UK personal data outside of the EEA/UK/Switzerland. These are required under European and UK data protection laws and are incorporated into our agreements.

Airwallex ensures that the recipient (and its jurisdiction) of personal data offers an adequate level of protection and security, for instance by incorporating the SCCs (or any equivalent contract issued by relevant authorities) into its agreements (where applicable) and/or adopting alternative measures required for the lawful transfer of personal data in accordance with applicable data protection laws, as well as a range of technical and organisational measures (described in more detail under the relevant heading below).

Airwallex's technical and organisational measures

We apply technical and organisational measures to protect the security of personal data. These include an information security management system aligned with ISO27001 and annually audited against SOC2 Type II as described below:

- ***A.5: Information security policies***
  Airwallex has implemented security policies and standards that are constantly reviewed in line with the overall direction of the organisation's information security practices. Risk

assessments are performed on a regular basis and agreed mitigating controls are included in the policies, standards and procedures to address security globally.

- ***A.6: Organization of information security***
  Airwallex's information security policies and standard assign responsibilities for information security related tasks. It ensures that the organisation has established a framework that can adequately implement and maintain information security practices within the organisation supported by senior leadership.

- ***A.7: Human resource security***
  Airwallex ensures individuals are screened before employment, makes sure that employees and contractors understand their responsibilities and addresses their responsibilities when they no longer hold that role – either because they've left the organisation or changed positions.

- ***A.8: Asset management***
  Airwallex identifies, classifies information assets to define the appropriate level of defence required and defines appropriate protection responsibilities for them. Endpoints are hardened, protected and monitored to help prevent the unauthorised disclosure, modification, removal or destruction of sensitive data.

- ***A.9: Access control***
  Policies and procedures for logical security are formally established and documented. User accounts belonging to Airwallex's employees and contractors are approved, added, modified, or disabled in a timely manner and are reviewed on a periodic basis.

- ***A.10: Cryptography***
  Airwallex deploys industry standard encryption technologies to protect business data and confidential information at rest and in transit and applies proper key management to the protection of its cryptographic keys.

- ***A.11: Physical and environmental security***
  Airwallex offices have implemented rigorous physical and environmental controls for its security. Airwallex uses security certified GCP and Aliyun data centers and follows its Supplier relationship management process and controls.

- ***A.12: Operations security***
  Airwallex applies management controls, operation controls and technological controls to protect business data and confidential information to provide for sustainable operation of business and application systems. Endpoints are protected against malware to mitigate the risk of infections, critical systems are logged and monitored, systems are hardening following CIS Benckmarks, periodically tested via automatic and manual means.

- ***A.13: Communications security***
  Airwallex networks are managed and controlled in order to protect information within systems and applications. Airwallex uses technology to perform endpoint verification, has implemented firewalls to segregate environments, has clear segregation between

production and non-production environments, access control lists, 2 factor authentication (i.e. software and hard token). Airwallex has also implemented strict endpoint controls for employees connecting to public networks (e.g. WFH arrangements) to consider the increased risk levels and to manage these risks. Airwallex also monitors its platforms to detect any anomalies that may present a threat to the company.

- ***A.14: System acquisition, development and maintenance (13 controls)***
  Airwallex has implemented a DevSecOps model and embedded security into the SDLC. It has integrated the security, availability and confidentiality into product design, and provides related functions to meet the user entities' requirements on security, availability and confidentiality. It has applied a secured change management process which encapsulates secure coding, configuration, scanning, patching monitoring and frequent testing.

- ***A.15: Supplier relationships (5 controls)***
  Before onboarding Subprocessors, Airwallex conducts an audit of the security and privacy practices of Subprocessors to ensure Subprocessors provide a level of security and privacy appropriate to their access to data and the scope of the services they are engaged to provide. Once Airwallex has assessed the risks presented by the Subprocessor, then subject to the engagement requirements the Subprocessor is required to enter into appropriate security, confidentiality and privacy contract terms.

- ***A.16: Information security incident management***
  Security incidents and unauthorized disclosures of customer data are communicated to customers, relevant legal and regulatory authorities, and others as required by law, contract, or at the advice of legal counsel, as per defined in the information security management and data breach standards."

- ***A.17: Information security aspects of business continuity management***
  Airwallex has established corresponding service cycles and service availability commitments to provide high availability of user entities' business and systems.

- ***A.18: Compliance***
  Airwallex has implemented compliance processes to guarantee it addresses internal requirements, such as policies and standards, and with external requirements, such as laws and regulations and contractual requirements to mitigate the risks of non-compliance and the penalties that come with that.

Your rights and choices

Please refer to Section 7 of our Global Privacy Policy.

Contact Us

If you would like to make any inquiries about our privacy policy, please contact us at:

- Airwallex privacy team: privacy@airwallex.com