

PRIVACY POLICY

Last updated March 2026

Thank you for choosing PingPong and its Group Companies (each as defined in our Terms and Conditions and hereinafter collectively "**Company**", "**we**", "**us**", and "**our**"). We are committed to protecting your personal information and your right to privacy. If you have any questions or concerns about our policy, or our practices with regards to your personal information, please contact us through the ways specified in Article 12.

When you visit our website to contact us or to use our services, you trust us with your personal information. We take your privacy very seriously. In this privacy policy, we seek to explain to you in the clearest way possible what information we collect, how we use it and what rights you have in relation to it. We hope you take some time to read through it carefully, as it is important. If there are any terms in this privacy policy that you do not agree with, please discontinue use of our website and our Services.

This privacy policy applies to all information collected through our website, and/or any related services, sales, marketing or events (we refer to them collectively in this privacy policy as the "**Services**").

Please read this privacy policy carefully as it will help you make informed decisions about sharing your personal information with us. A PDF version of this privacy policy can be found here.

For residents of the European Economic Area and Switzerland, personal information is processed by or on behalf of the controller:

PingPong Europe SA
Rue du Laboratoire 9
Luxembourg L-1911
Luxembourg

For residents of the United Kingdom, personal information is processed by or on behalf of the controller:

PingPong Payment (UK) Limited
78 Cannon Street
London, EC4N 6NP
United Kingdom

For residents of the United States of America, personal information is processed by or on behalf of the controller:

PingPong Global Solutions Inc.
27 W. 24th Street, Suite 704
New York, New York 11010
The United States of America

1. WHAT INFORMATION DO WE COLLECT?

We may collect one or more of the following categories of personal information about you when you visit our website, use or register for our Services, request additional information about our Services, or otherwise interact with us.

Category of Personal Information Collected	Types of Personal Information Collected	Sources of Personal Information Collected	Business Purpose for Collection of Personal Information
Identifiers	Name (First, Last, Maiden, if applicable), Address, Prior Addresses, Phone Number, Email Address, Business Contact Information, Business Associates, Corporate Affiliations, Account Username/Password, Payment Information, Credit Card Number, Banking Information (including account information and statements), IP Address.	Directly from you, cookies and other tracking technologies, Public Sources.	Provide our Services, Identification, Communications, Security, Legal, Compliance and Regulatory Obligations, Marketing Purposes.
Protected Characteristics under California or Federal Laws	Age, Gender, National Origin	Directly from you.	Provide our Services, Identification, Legal, Compliance and Regulatory Obligations.
Sensitive Personal Information	Driver's License Number, Passport Number, Precise Geolocation	Directly from you, Cookies and other tracking technologies.	Provide our Services, Identification, Legal, Compliance and Regulatory Obligations.
Commercial Information	Purchase History, Invoices	Directly from you.	Provide our Services, Identification, Legal, Compliance and Regulatory Obligations.
Biometric Information	Photos, Fingerprints, Photo or Video "Selfies"	Directly from you.	Provide our Services, Identification, Legal, Compliance and Regulatory Obligations.

Internet / Network Activity	Device ID, and Device Settings (e.g., language preference, time zone), Login Information, Login History, Browser Type and Version, Browser Plug-In Types and Versions, Operating System and Platform, Google Analytics Cookies, and Information about your visit to our website.	Cookies and other tracking technologies.	Provide our Services, Identification, Legal, Compliance and Regulatory Obligations.
Professional & Employment Information	Business, Job Title, Business Associates, Corporate Affiliations, Information from your Curriculum Vitae (CV).	Directly from you.	Provide our Services, Identification, Legal, Compliance and Regulatory Obligations.
Audio, Electronic, Visual, Thermal, Olfactory or Similar Information	Call Center Recordings.	Directly from you.	Provide our Services, Identification, Legal, Compliance and Regulatory Obligations.

We do not collect the following categories of personal information about our customers: education information, defined as information that is not publicly available personally identifiable information as defined in the United States Family Educational Rights and Privacy Act (20 U.S.C. Sec. 1232g; 34 C.F.R. Part 99); or inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

We process this personal information on the following legal bases:

- **Consent:** We may process your personal information if you have given us specific consent to use it for a specific purpose.
- **Legitimate Interests:** We may process your personal information when it is reasonably necessary to achieve our legitimate business interests.
- **Performance of a Contract:** Where we have entered into a contract with you, we may process your personal information to fulfill the terms of our contract.
- **Legal Obligations:** We may disclose your information where we are legally required to do so in order to comply with applicable law, governmental requests, a judicial proceeding, court order, or legal process, such as in response to a court order or a

subpoena (including in response to public authorities to meet national security or law enforcement requirements).

- **Vital Interests:** We may disclose your information where we believe it is necessary to investigate, prevent, or take action regarding potential violations of our policies, suspected fraud, situations involving potential threats to the safety of any person and illegal activities, or as evidence in litigation in which we are involved.

Automated Decision-Making/Profiling: Please note, PingPong does not utilize automated individual decision-making (making a decision solely by automated means without any human involvement) or profiling (automated processing of personal data to evaluate certain things about an individual).

2. DO WE USE COOKIES AND OTHER TRACKING TECHNOLOGIES?

In Short: We may use cookies and other tracking technologies to collect and store your information.

We may use cookies and similar tracking technologies (like web beacons and pixels) to access or store information. Specific information about how we use such technologies and how you can refuse certain cookies is set out in our Cookie Policy.

Most Web browsers are set to accept cookies by default. If you prefer, you can usually choose to set your browser to remove cookies and to reject cookies. If you choose to remove cookies or reject cookies, this could affect certain features or services of our Services.

3. HOW DO WE USE YOUR INFORMATION?

In Short: We process your information for purposes based on legitimate business interests, the fulfillment of our contract with you, compliance with our legal obligations, and/or your consent.

We use personal information collected via our website or Services for a variety of business purposes described below. We process your personal information for these purposes in reliance on our legitimate business interests, in order to contact you, enter into or perform a contract with you, with your consent, and/or for compliance with our legal obligations. If you choose not to provide information, we may be unable to provide services to you or the quality of services you receive may be affected. We indicate the specific processing grounds we rely on next to each purpose listed below.

Purpose of Collection and Disclosure	Detailed Scope of Processing Activities	Lawful Basis for Processing
Account Creation & Logon	To facilitate the account creation process, enable secure logon, and manage user accounts to keep our platforms operational and services safe and secure.	Contractual Necessity; Legitimate Interests (to ensure platform security and fraud prevention).
Service Delivery & Provision	To provide, deliver, and perform the services you have requested, ensuring the integrity and functionality of our services. We may use your information to improve our services and to ensure that they are presented in the most effective manner.	Contractual Necessity; Legal Obligation; Legitimate Interests (preventing misuse or breaches of service).
Identity Verification (KYC/AML)	To verify your identity during onboarding and throughout our relationship to comply with mandatory "Know Your Customer" (KYC) obligations and anti-money laundering (AML) laws.	Legal Obligation; Contractual Necessity; Legitimate Interests (to detect, prevent, and investigate financial crimes).
Fraud Prevention & Risk Management	To prevent, detect, or protect against actual or suspected fraud, unauthorized transactions, claims, liability, and financial or other crimes (including conducting or co-operating with investigations); To recover amounts owed (including insurance claims); To allow third parties/financial institutions to recover money sent in error or due to fraud; To prevent and manage incidents of abusive/aggressive behaviour towards our employees.	Legitimate Interests; Legal Obligation
Communication & Support	We contact you regarding our products and services, and use your information to respond to inquiries, troubleshoot, and solve potential issues you might encounter while using our Services.	Contractual Necessity; Legitimate Interests (to maintain service integrity and resolve issues).

Marketing & Analytics	Personalising marketing messages to make them relevant and interesting; Measuring/understanding advertising effectiveness and delivering relevant advertising; Providing information about similar products/services that may interest you; Holding promotions and competitions for our products or services.	Legitimate Interests (to inform customers about relevant services and analyze advertising effectiveness); Consent (where required by law, including for personalized location-based updates).
Policy Enforcement	To enforce our terms, conditions, and policies for Business Purposes, Legal Reasons, and Contractual Obligations; To verify information provided to us; To enforce our Customer Agreement with you; To investigate, manage, and resolve complaints.	Contractual Necessity; Legal Obligation.
Legal Requests & Compliance	To comply with legal and/or regulatory requirements, including responding to requests from public and government authorities (possibly outside your country of residence) upon demonstration of lawful authority; To comply with obligations to determine your tax status and compliance with associated tax regulations.	Legal Obligations; Legitimate Interests (to protect our business, customers, and employees from harm).
System Improvement & Development	We process your personal data to undertake system or product development, maintain and improve our services, and help third-party suppliers improve the services they provide to us.	Legitimate Interests (to maintain, develop, and optimize our platform performance and service effectiveness).

4. WILL YOUR INFORMATION BE SHARED WITH ANYONE?

In Short: We may sell or share your personal information as those terms are defined under applicable data protection laws, with your consent, to comply with laws, to provide you with services, to respond to your inquiries, to protect your rights, or to fulfill business obligations.

With your consent, we may share your personal information with third parties. Otherwise, we may sell or share your personal information with the following categories of recipients and in the following situations:

- **Vendors, Consultants, Other Third-Party Service Providers, and Affiliate Companies.** We may share your data with third party vendors, service providers, contractors or agents who perform services for us or on our behalf and require access to such information to do that work. We work with third parties that provide us with engine or application development and/or processing services; information systems hosting, infrastructure, maintenance, backup, storage, security, support, and other information

technology-related services; advertising, marketing, and related analytics services; promotion, distribution, resale, and support services related to our products and services; consulting and other technical and/or business services, including to our professional advisors, attorneys, and auditors, which may require access to information about you to perform such services on our behalf. We share your information with these service providers only for our business purposes pursuant to written contracts. Our contracts with these third-party service providers require protection of your information consistent with this privacy policy, and require that they retain, use, and disclose your information only as necessary to provide the services in accordance with such contracts.

- **Legal and Regulatory Authorities.** We may share information about you with a third party if we believe that sharing such information is reasonably necessary to (a) comply with any applicable law, regulation, legal process or governmental request, including to meet national security requirements, (b) enforce our agreements, policies and terms of service, or to exercise or defend any legal claims, (c) protect the security or integrity of our products and services, and (d) protect us, our customers, employees or other persons from harm or illegal activities.
- **Business Transfers.** We may share or transfer your information in connection with, or during negotiations of, any merger, sale of company assets, financing, or acquisition of all or a portion of our business by another company.
- **Third Party Advertisers.** We may sell your personal information to third parties for the purposes of engaging in targeted advertisements.

5. DO WE ENGAGE IN CROSS-BORDER DATA TRANSFERS?

In Short: We may transfer your personal information to a third party that is located in a jurisdiction other than the one from which we collected your personal information, including to countries that have not been deemed to have an adequate level of protection for the rights and freedoms of data subjects.

For the EU/UK/Switzerland:

We may process your personal data on servers located outside of the EEA, Switzerland, and the UK for the purposes described in this policy. This includes processing and storing your personal data in our facilities and servers in the United States or in countries or territories where our affiliates and partners or our vendors and service providers are located. While data protection law varies by country, and these countries may not offer the same level of data protection as your home country, we apply the protections described in this policy to your Personal Data regardless of where it is processed. When transferring Personal Data outside of the EEA, Switzerland, or the UK, we rely on valid transfer mechanisms to comply with applicable data protection law, such as:

- We rely on the European Commission's adequacy decisions and the UK Secretary of State's adequacy regulations pursuant to Article 45(1) EU and UK GDPR ("**GDPR**") when transferring your Personal Data to any country that has been considered to provide an adequate level of protection.
- For other jurisdictions, we rely on the Standard Contractual Clauses as approved by the European Commission pursuant to Article 46(2)(c) GDPR ("**SCCs**") and on the UK International Data Transfer Addendum to the SCCs.

For more information or to obtain a copy of the appropriate safeguards we have in place when transferring personal data, please contact us at dpo@pingpongx-eu.com.

6. HOW LONG DO WE KEEP YOUR INFORMATION?

***In Short:** We keep your personal information only for as long as necessary to fulfill the purposes outlined in this privacy policy unless otherwise required by law.*

We will only keep your personal information for as long as it is necessary to fulfill the purposes for which it was collected, including for the purposes of satisfying any legal, regulatory, accounting, or reporting requirements. If we collect any biometric information about you, we will not store that information for longer than required under state law, and we will destroy all copies of such biometric information after the retention period set by state law from the date of collection.

7. HOW DO WE KEEP YOUR INFORMATION SAFE?

***In Short:** We aim to protect your personal information through a system of organizational and technical security measures.*

We have implemented appropriate administrative, technical, and organizational security measures designed to protect the security of any personal information we process. However, please also remember that we cannot guarantee that the internet itself is 100% secure. Although we will do our best to protect your personal information, transmission of personal information to and from our Services is at your own risk. You should only access the services within a secure environment.

8. DO WE COLLECT INFORMATION FROM MINORS?

***In Short:** We do not knowingly collect data from or market to children under 18 years of age.*

We do not knowingly solicit data from or market to children under 18 years of age. By using the Services, you represent that you are at least 18 or that you are the parent or guardian of such a minor and consent to such minor dependent's use of the Services. If we learn that personal information from users less than 18 years of age has been collected, we will deactivate the account and take reasonable measures to promptly delete such data from our records. If you become aware of any data we have collected from children under age 18, please contact us through the ways specified in Article 12.

9. WHAT ARE YOUR PRIVACY RIGHTS?

***In Short:** In some regions, you have rights that allow you greater access to and control over your personal information. You may review, change, or terminate your account at any time.*

Depending upon where you are located, certain choices and rights may be available to you under applicable data protection laws, including the right to request access to your personal information or to have your personal information deleted.

If you have questions or comments about your privacy rights, you may email us through the ways specified in Article 12.

"Do-Not-Track": Most web browsers and some mobile operating systems and mobile applications include a Do-Not-Track ("DNT") feature or setting you can activate to signal your privacy preference not to have data about your online browsing activities monitored and collected. No uniform technology standard for recognizing and implementing DNT signals has been finalized. As such, we do not currently respond to DNT browser signals or any other mechanism that automatically communicates your choice not to be tracked online.

"Shine the Light" and "Eraser" Laws: Residents of the State of California may request a list of all third parties to which we have disclosed certain information during the preceding year for those third parties' direct marketing purposes.

California Consumer Privacy Act (CCPA)/California Privacy Rights Act (CPRA): The CCPA, as amended by the CPRA, provides California residents and/or their authorized agents with specific rights regarding the collection and storage of their personal information.

Your Right to Know: California residents have the right to request that we disclose the following information to you about our collection and use of your personal information over the past twelve (12) months. We may ask you to provide certain information to identify yourself so that we may compare it with our records in order to verify your request. Upon verification, we will disclose to you:

1. The categories of personal information we have collected about you.
2. The categories of sources for the personal information we have collected about you.
3. The specific pieces of personal information we have collected about you.
4. Our business or commercial purpose for collecting or selling your personal information.
5. The categories of third parties to whom we have sold or shared your personal information, if any, and the categories of personal information that we have shared with each third-party recipient.

Your Right to Opt-Out of Sale or Sharing of Personal Information: California residents have the right to opt-out of the sale of their personal information by submitting a request as directed on the homepage of our website.

Please note that we do not knowingly sell the personal information of any individuals under the age of 16.

Where we are sharing your personal information with third parties for the purposes of cross-context behavioral advertising or profiling, you may opt-out of such sharing at any time by submitting a request as directed on the homepage of our website or by contacting us using the information in the "Contact Us" section below.

Your Right to Limit Use of Sensitive Personal Information: California residents have the right to request that we limit our use of any sensitive personal information to those uses which are necessary to perform the Services or for other specifically-enumerated business purposes under the CCPA, as amended by the CPRA.

Your Right to Delete: California residents have the right to request that we delete any of the personal information collected from you and retained by us, subject to certain exceptions. We

may ask you to provide certain information to identify yourself so that we may compare it with our records in order to verify your request. Once your request is verified and we have determined that we are required to delete the requested personal information in accordance with the CCPA, we will delete, and direct our third-party service providers to delete, your personal information from their records. Your request to delete personal information that we have collected may be denied if we conclude it is necessary for us to retain such personal information under one or more of the exceptions listed in the CCPA.

Your Right to Correct: Under the CCPA, as amended by the CPRA, California residents have the right to request that we correct any inaccurate personal information we maintain about you, taking into account the nature of the personal information and the purposes for which we are processing such personal information. We will use commercially reasonable efforts to correct such inaccurate personal information about you.

Non-Discrimination: You will not receive any discriminatory treatment by us for the exercise of your privacy rights conferred by the CCPA, as amended by the CPRA.

Verifying Your Request: Only you, or a person that you authorize to act on your behalf, may make a request related to your personal information. In the case of access and deletion, your request must be verifiable before we can fulfill such request. Verifying your request will require you to provide sufficient information for us to reasonably verify that you are the person about whom we collected personal information or a person authorized to act on your behalf. We will only use the personal information that you have provided in a verifiable request in order to verify your request. We cannot respond to your request or provide you with personal information if we cannot verify your identity or authority. Please note that we may charge a reasonable fee or refuse to act on a request if such request is excessive, repetitive, or manifestly unfounded.

Opting out of email marketing: You can unsubscribe from our marketing email list or request not to be contacted by us in the future at any time by clicking on the unsubscribe link in the emails that we send or by contacting us using the details provided below. You will then be removed from the marketing email list, and/or will not be contacted – however, we will still need to send you service-related emails that are necessary for the administration and use of your account. To otherwise opt-out, you may:

- Note your preferences when you register an account with the site.
- Access your account settings and update preferences.
- Contact us using the contact information provided.

10. DO WE HAVE CONTROL OVER ANY THIRD-PARTY LINKS?

In Short: No. We do not have the ability to control any information provided under third-party links.

We may provide links to other websites or resources provided by third parties. These links are provided for your convenience only. We have no control over the content of those websites or resources and accept no responsibility for them or for any loss or damage that may arise from your use of them. If you decide to access third-party links on the Sites, you do so entirely at your own risk and subject to the terms and conditions of those websites.

11. DO WE MAKE UPDATES TO THIS POLICY?

In Short: Yes, we will update this policy as necessary to stay compliant with relevant laws.

We may update this privacy policy from time to time. The updated version will be indicated by an updated "Revised" date, and the updated version will be effective as soon as it is accessible. If we make material changes to this privacy policy, we may notify you either by prominently posting a notice of such changes or by directly sending you a notification. We encourage you to review this privacy policy frequently to be informed of how we are protecting your information.

12. HOW CAN YOU CONTACT US ABOUT THIS POLICY?

If you have questions or comments about this privacy policy or if you would like to exercise any of your privacy rights and you are a resident in:

- The European Economic Area or Switzerland, the "data controller" of your personal information is PingPong Europe SA. You can contact us directly regarding the processing of your information, by email at dpo@pingpongx-eu.com, or by post to the address set forth below. If you believe we have not adequately resolved any issues, you may contact the Supervisory Authority concerned.

PingPong Europe SA
Data Protection Department
Rue du Laboratoire 9
L-1911
Luxembourg

- The United Kingdom, the "data controller" of your personal information is PingPong Payment (UK) Limited. You can contact us directly regarding the processing of your information, by email at dpo-uk@pingpong-uk.com, or by post to the address set forth below. If you believe we have not adequately resolved any issues, you may contact the Supervisory Authority concerned.

PingPong Payment (UK) Limited
Data Protection Department Cannon Street
London, EC4N 6NP
United Kingdom

- The United States of America, the "data controller" of your personal information is PingPong Global Solutions Inc. You can contact us directly regarding the processing of your information, by email at privacy@pingpongx.us, or by post to the address set forth below. If you believe we have not adequately resolved any issues, you may contact the Supervisory Authority concerned.

PingPong Global Solutions Inc.
27 W 24th Street Suite 704
NY, NY 11010
The United States of America

- Any country other than those listed in the immediately preceding bullet, the "data controller" of your personal information is the PingPong Group member company with

which you contract pursuant to our Terms and Conditions. You can contact us directly regarding the processing of your information by email at privacy@pingpongx.us or by post at the address set across from the relevant PingPong Group entity in your Terms and Conditions.

EXHIBIT A: COUNTRY-SPECIFIC TERMS

The following terms apply to residents of the United States of America, and shall be deemed to be included in and form a part of the PingPong Privacy Policy. To the extent any conflict exists between these country-specific terms and the PingPong Privacy Policy, the provisions of these country-specific terms will prevail for applicable Customers.

Clause 4 is replaced as follows:

“ 4. WILL YOUR INFORMATION BE SHARED WITH ANYONE ?

***In Short:** We may sell or share your personal information as those terms are defined under applicable data protection laws, with your consent, to comply with laws, to provide you with services, to respond to your inquiries, to protect your rights, or to fulfill business obligations.*

With your consent, we may share your personal information with third parties. Otherwise, we may sell or share your personal information with the following categories of recipients and in the following situations:

Third Party	Purpose
Our corporate affiliates	To facilitate or support us in providing the Services to you, we may share your personal information within our group of companies. All PingPong group companies may only use your personal information in accordance with the relevant Intra-Group contracts governing such processing and for the purposes set out in this Policy.
Banks and other financial institutions	Our Services may be offered to you in conjunction with or facilitated by other financial institutions or other bank partners. Such partners may have access to your personal information but only to the extent required to enable you to use our or their products and services or otherwise as authorised or requested by you.
Third party service providers	<p>We may share your data with third party vendors, service providers, contractors or agents who perform services for us or on our behalf and require access to such information to do that work, such as:</p> <ul style="list-style-type: none"> • Cloud Storage and IT Infrastructure Providers: To provide hosting, security, maintenance, and technical support to ensure the stability and reliability of our services. • Verification Service Providers: To verify your identity, address, and credentials in compliance with "Know Your Customer" (KYC) and Anti-Money Laundering (AML) regulatory requirements. • Fraud Prevention Agencies: Specialized entities that assist us in identifying, mitigating, and preventing fraudulent transactions to

	<p>protect our users and our financial ecosystem.</p> <ul style="list-style-type: none"> • Business Partners: Who assist us in delivering specific products or features. <p>We share your information with these service providers only for our business purposes pursuant to written contracts. Our contracts with these third-party service providers require protection of your information consistent with this privacy policy, and require that they retain, use, and disclose your information only as necessary to provide the services in accordance with such contracts.</p>
Regulators, law enforcement agencies, tax authorities and public authorities	We may share information about you with a third party if we believe that sharing such information is reasonably necessary to (a) comply with any applicable law, regulation, legal process or governmental request, including to meet national security requirements, (b) enforce our agreements, policies and terms of service, or to exercise or defend any legal claims, (c) protect the security or integrity of our products and services, and (d) protect us, our customers, employees or other persons from harm or illegal activities.
Beneficiaries	that receive limited information when you initiate a payment transaction
Business Transfers	We may share or transfer your information in connection with, or during negotiations of, any merger, sale of company assets, financing, or acquisition of all or a portion of our business by another company.
With Your Consent	In some cases, we may share your information with other third parties when you provide explicit consent to do so.

Personal data collected by us is primarily stored and processed on servers located in the United States. However, as a global provider of money transfer and multi-currency services, we may process and store your personal data in jurisdictions other than your country of residence when necessary. This is strictly to facilitate the performance of our services and comply with our legal obligations.

We are committed to implementing appropriate technical and organizational safeguards to ensure your data remains protected according to the standards required by applicable law, regardless of where it is processed. When transferring your data to jurisdictions that may not provide the same level of data protection as your home country, we ensure that your data is adequately protected by implementing appropriate safeguards."

US Consumer Privacy Notice (GLBA)

The following Consumer Privacy Notice applies to you if you are an individual who resides in the United States and obtains financial services from PingPong primarily for your own personal, family, or household purposes.

Who is providing this notice? PingPong Global Solutions Inc and its affiliates that provide consumer services in the U.S.

Federal law gives consumers the right to limit some but not all sharing. Federal law also requires us to tell you how we collect, share, and protect your personal information. Please read this notice carefully to understand what we do.

1. What Personal Information We Collect

The types of personal information we collect and share depend on the product or service you have with us. This information can include:

- Social Security Number
- Contact details
- Account balances and transaction history
- Payment, transaction, and purchase information and history, and related data to detect fraud and prevent loss
- Credit reports and other information necessary to facilitate credit card issuing

When you are no longer our customer, we continue to share your information as described in this notice.

2. How does PingPong collect my personal information?

We collect your personal information, for example, when you

- open a payment account;
- ask PingPong to process a payment for goods or services;
- provide bank account information to PingPong.

We also collect your personal information from others, such as affiliates or other companies.

3. How We Protect Your Personal Information

To protect your personal information from unauthorized access, destruction, loss, alteration, or misuse, we use security measures to comply with federal law. These measures include computer safeguards and secured files and buildings. We impose access controls along with ongoing monitoring to prevent data misuse, and we require our service providers to take similar steps to protect your information.

4. Reasons We Share Your Personal Information & How to Limit Sharing

All financial companies need to share customers' personal information to run their everyday business. We list the reasons financial companies can share their customers' personal information below; the reasons PingPong chooses to share; and whether you can limit this sharing.

Reasons we can share your personal information	Does PingPong share?	Can you limit this sharing
For our everyday business purposes – such as to process your transactions, detect fraud and prevent loss for you, us, and Financial Partners, maintain your account(s), respond to court orders and legal investigations.	Yes	No
For our marketing purposes - to offer our products and services to you.	Yes	Yes
For nonaffiliates to market to you.	No	We don't share

Federal law gives you the right to limit only

- sharing for affiliates' everyday business purposes — information about your creditworthiness
- affiliates from using your information to market to you
- sharing with nonaffiliates to market to you.

State laws and individual companies may give you additional rights to limit sharing. See the Other Important Information section below for more information on your rights under state law.

To limit our sharing or if you have questions? Contact us at privacy@pingpongx.us.

5. Other Important Information

State laws and individual companies may give you additional rights to limit sharing. See the Other Important Information section below for more information on your rights under state law.

Vermont:

If your account with us is associated with a Vermont billing address, we will not disclose information about your creditworthiness to our affiliates and will not disclose your personal information, financial information, credit report, or health information to nonaffiliated third parties to market to you, other than as permitted by Vermont law, unless you authorize us to make those disclosures. For joint marketing, we will only disclose your name, contact information, and information about your transactions.

California:

If your account with us is associated with a California billing address, we will not disclose Personal Data we collect about you except to the extent permitted under California law. For instance, we may disclose your Personal Data as necessary to process transactions or provide products and services you request, at your instruction, as required for institution risk control, and to safeguard against fraud, identity theft, and unauthorized transactions.

UK/EEA/Switzerland Area Specific Terms

The following terms apply to residents of the European Economic Area and the United Kingdom, and shall be deemed to be included in and form a part of the PingPong Privacy Policy. To the extent any conflict exists between these country-specific terms and the PingPong Privacy Policy, the provisions of these country-specific terms will prevail for applicable Customers.

The following language is added to Clause 2:

"We use cookies and similar technologies to operate and administer our services, and improve your experience. We store some of the information described in this Policy with cookies, for example, to help maintain your preferences across sessions if you're not logged in, or to assist with authentication and customer support. For details about our use of cookies, please read our Cookie Notice.

Clause 4 is replaced as follows:

" 4. WILL YOUR INFORMATION BE SHARED WITH ANYONE?"

***In Short:** We may sell or share your personal information as those terms are defined under applicable data protection laws, with your consent, to comply with laws, to provide you with services, to respond to your inquiries, to protect your rights, or to fulfill business obligations.*

With your consent, we may share your personal information with third parties. Otherwise, we may sell or share your personal information with the following categories of recipients and in the following situations:

Third Party	Purpose
Our corporate affiliates	To facilitate or support us in providing the Services to you, we may share your personal information within our group of companies. All PingPong group companies may only use your personal information in accordance

	with the relevant Intra-Group contracts governing such processing and for the purposes set out in this Policy.
Banks and other financial institutions	Our Services may be offered to you in conjunction with or facilitated by other financial institutions or other bank partners. Such partners may have access to your personal information but only to the extent required to enable you to use our or their products and services or otherwise as authorised or requested by you.
Third party service providers	<p>We may share your data with third party vendors, service providers, contractors or agents who perform services for us or on our behalf and require access to such information to do that work, such as:</p> <ul style="list-style-type: none"> • Cloud Storage and IT Infrastructure Providers: To provide hosting, security, maintenance, and technical support to ensure the stability and reliability of our services. • Verification Service Providers: To verify your identity, address, and credentials in compliance with "Know Your Customer" (KYC) and Anti-Money Laundering (AML) regulatory requirements. • Fraud Prevention Agencies: Specialized entities that assist us in identifying, mitigating, and preventing fraudulent transactions to protect our users and our financial ecosystem. • Business Partners: Who assist us in delivering specific products or features. <p>We share your information with these service providers only for our business purposes pursuant to written contracts. Our contracts with these third-party service providers require protection of your information consistent with this privacy policy, and require that they retain, use, and disclose your information only as necessary to provide the services in accordance with such contracts.</p>
Regulators, law enforcement agencies, tax authorities and public authorities	We may share your Personal Data, including information about your interaction with our Services, with government authorities, industry peers, or other third parties in compliance with the law (i) if required to do so to comply with a legal obligation, or in the good faith belief that such action is necessary to comply with a legal obligation, (ii) to protect and defend our rights or property, (iii) if we determine, in our sole discretion, that there is a violation of our terms, policies, or the law; (iv) to detect or prevent fraud or other illegal activity; (v) to protect the safety, security, and integrity of our products, employees, users, or the public, or (vi) to protect against legal liability.
Beneficiaries	that receive limited information when you initiate a payment transaction
Business Transfers	We may share or transfer your information in connection with, or during negotiations of, any merger, sale of company assets, financing, or acquisition of all or a portion of our business by another company.
With Your Consent	In some cases, we may share your information with other third parties

	when you provide explicit consent to do so.
--	---

Personal data collected by us is primarily stored and processed on servers located in the United States. However, as a global provider of money transfer and multi-currency services, we may process and store your personal data in jurisdictions other than your country of residence when necessary. This is strictly to facilitate the performance of our services and comply with our legal obligations.

We are committed to implementing appropriate technical and organizational safeguards to ensure your data remains protected according to the standards required by applicable law, regardless of where it is processed. When transferring your data to jurisdictions that may not provide the same level of data protection as your home country, we ensure that your data is adequately protected by implementing appropriate safeguards."

The following language is added to **Clause 7**:

We implement commercially reasonable technical, administrative, and organizational measures designed to protect Personal Data from loss, misuse, and unauthorized access, disclosure, alteration, or destruction. However, no Internet or email transmission is ever fully secure or error free. Therefore, you should take special care in deciding what information you provide to the Services. In addition, we are not responsible for circumvention of any privacy settings or security measures contained on the Service, or third-party websites.

The following language is added to **Clause 9**:

"You have the following statutory rights in relation to your Personal Data:

- Access your personal data and information relating to how it is processed.
- Delete your personal data from our records.
- Rectify or update your personal data.
- Transfer your personal data to a third party (right to data portability).
- Restrict how we process your personal data.
- Withdraw your consent—where we rely on consent as the legal basis for processing.
- Lodge a complaint with your local data protection authority (see below).

You have the following rights to object:

- Object to our processing of your personal data for direct marketing.
- Object to how we process your personal data when our processing is based on legitimate interests.

You can exercise some of these rights through your PingPong account. If you are unable to exercise your rights through your account, please submit your request to dpo@pingpongxeu.com

We hope that we are able to address any questions or concerns you may have. If you have any unresolved complaints with us or our Data Protection Officer:

- If you reside in the European Economic Area, you can reach out to the Luxembourg Data Protection Commission as our lead supervisory authority, or your local supervisory authority.
- If you reside in the UK, you can reach out to the Information Commissioner's Office.
- If you reside in Switzerland, you can reach out to the Federal Data Protection and Information Commissioner."

Clause 13 is added as follows:

We'll retain your personal data for only as long as we need in order to provide our services to you, or for other legitimate business purposes such as resolving disputes, safety and security reasons, or complying with our legal obligations. How long we retain personal data depends on the type of data, how we use it, and, in many cases, your settings:

- **Information we retain until you delete it:** Some of our services allow you to delete Personal Data stored in your account. Once you choose to delete personal data, we will remove it from our systems within 30 days unless we need to retain it for longer as described below, or it has already been de-identified and disassociated from your account.
- **Information we delete automatically:** In some cases, personal data will be deleted automatically.
- **Information we retain for longer for legitimate security, safety, or legal reasons:** In some cases, we need to retain personal data for longer even after you delete it, for example because we are legally required to, to address fraud and abuse, for security reasons, or for financial record-keeping purposes. For instance:
 - If specific content, or your account, is banned because of violations of our [usage policies](#), we may retain that data to protect our services from fraud, abuse, or other violations of our policies;
 - If we are legally required to retain your data (for instance, we receive a lawful subpoena), then we may retain it for the duration of the relevant legal or regulatory obligation;
 - When we are a party to a financial transaction, we may retain payment and transaction-related information to meet our accounting, dispute resolution, and regulatory compliance purposes;

- When you ask us to delete your personal data, we retain the audit record of the erasure request to be able to verify that we have complied with the request.
- For example, we keep KYC documentation for up to five (5) years after last usage of your account, at which time it will be deleted.

In determining these retention periods, we consider a number of factors, such as:

- Our purpose for processing personal data (such as whether we need to retain it to provide our services);
- The amount, nature, and sensitivity of the information;
- The potential risk of harm from unauthorized use or disclosure;
- Any legal requirements that we are subject to.