A colorful squares with different shapes

AI-generated content may be incorrect.

**Privacy Policy Template for   
Business Owners**

**A Starting Point for Your Policy Development Process**

Creating a privacy policy that complies with global privacy laws requires a comprehensive approach, addressing the various requirements of different regulations like GDPR, CCPA/CPRA, LGPD, PIPEDA, and others. Below is a categorized online web privacy policy, structured to highlight compliance with these laws.

**DISCLAIMER:** THIS PRIVACY POLICY TEMPLATE (“TEMPLATE”) PROVIDED BY COALITION, INC. AND ITS SUBSIDIARIES AND AFFILIATES, AS APPLICABLE (COLLECTIVELY, “COALITION") IS OFFERED FOR GENERAL INFORMATIONAL AND ILLUSTRATIVE PURPOSES ONLY. THIS TEMPLATE IS DESIGNED TO SERVE AS A STARTING POINT OR FRAMEWORK AND IS NOT INTENDED TO BE A COMPLETE, EXHAUSTIVE, OR DEFINITIVE SOLUTION FOR ANY SPECIFIC SITUATION OR LEGAL REQUIREMENT.

COALITION IS NOT PROVIDING PROFESSIONAL, BUSINESS OR ANY OTHER EXPERT ADVICE THROUGH THE PROVISION OR USE OF THIS TEMPLATE. YOU SHOULD CONSULT WITH QUALIFIED PROFESSIONALS (E.G., LICENSED ATTORNEYS, BUSINESS ADVISORS) IN YOUR OPERATING JURISDICTIONS TO ENSURE THAT THIS TEMPLATE ACCURATELY REFLECTS YOUR SPECIFIC CIRCUMSTANCES AND IS FULLY COMPLIANT WITH ALL APPLICABLE LAWS BEFORE RELYING ON OR IMPLEMENTING ANY PART OF THIS TEMPLATE.

COALITION DOES NOT WARRANT THAT THIS TEMPLATE WILL MEET YOUR SPECIFIC REQUIREMENTS, BE ERROR-FREE, OR THAT ANY DEFECTS WILL BE CORRECTED. COALITION MAKES NO GUARANTEES REGARDING THE EFFECTIVENESS, APPLICABILITY, OR LEGAL COMPLIANCE OF THIS TEMPLATE FOR YOUR PARTICULAR USE CASE AND DISCLAIMS ANY DUTY TO UPDATE THIS TEMPLATE. BY ACCESSING, DOWNLOADING, OR USING THIS TEMPLATE, YOU ACKNOWLEDGE AND AGREE THAT:

* YOU ARE SOLELY RESPONSIBLE FOR REVIEWING, UNDERSTANDING, ADAPTING, MODIFYING, AND VERIFYING THE ACCURACY, COMPLETENESS, AND LEGAL COMPLIANCE OF THIS TEMPLATE FOR YOUR SPECIFIC NEED(S) AND JURISDICTION(S).
* YOU ASSUME ALL RISKS ASSOCIATED WITH THE USE OF THIS TEMPLATE, INCLUDING BUT NOT LIMITED TO THE RISK OF ERRORS, OMISSIONS, INACCURACIES, OR LEGAL NON-COMPLIANCE.
* YOU UNDERSTAND THAT LAWS AND REGULATIONS CHANGE FREQUENTLY, AND THIS TEMPLATE MAY NOT BE UP-TO-DATE OR APPLICABLE IN ALL JURISDICTIONS.

**Document Key**

* Policy Text
* **Notes** (to be **deleted**)
* **Placeholder Text *(to be changed)***
* **Legal Basis** (to be **deleted**)

**Note:** below is an example introductory paragraph. Identify the jurisdictions in which your organization operates and include the applicable laws that form the basis of your privacy policy below.

# [Your Company Name] Online Privacy Policy

## Last Updated: [Insert Date Here] Effective Date: [Insert Date Here]

At **[Your Company Name]**, we are committed to protecting your privacy and personal data. This Privacy Policy (“Policy”) explains how we collect, use, disclose, and protect your personal data when you visit our website, **[Insert Your Website URL]**, and use our services. We comply with global privacy laws, including but not limited to:

* **General Data Protection Regulation (GDPR)** (UK, EU and EEA)
* **California Consumer Privacy Act (CCPA) / California Privacy Rights Act (CPRA)** (California, US)
* **Lei Geral de Proteção de Dados (LGPD)**(Brazil)
* **Personal Information Protection and Electronic Documents Act (PIPEDA)** (Canada)
* **Act on the Protection of Personal Information (APPI)** (Japan)
* **Australian Privacy Principles (APPs) under the Privacy Act 1988** (Australia)

By using our website, you agree to the collection and use of personal data in accordance with this Policy.

**Note:** This section provides contact information for your organization as it relates to processing of data.

## 1. Introduction and Scope

This Policy applies to all personal data processed by **[Your Company Name]** in connection with our services and website visitors.

**Our Contact Details:** **[Your Company Name] [Your Company Address] [Your Company Email Address] [Your Company Phone Number] [Link to Contact Form, if applicable]**

**Data Protection Officer (DPO) / Privacy Contact** (if applicable)**:** **[Name of DPO / Privacy Contact] [DPO / Privacy Contact Email Address]**

We encourage you to read this Policy carefully to understand our practices regarding your data and how we will treat it.

## 2. Information We Collect

We collect various types of information for different purposes to provide and improve our services to you. We only collect data that is necessary for the stated purposes.

**Note**: This section explains the types of information collected from a user when visiting an organization’s website or using their services

#### 2.1. Personal Data

This includes information that can be used to identify you directly or indirectly. The categories of personal data we may collect include:

**Note**: This section is for data that is provided directly by your organization. Update the categories of personal data below as appropriate.

* **Identifiers:** Name, email address, postal address, phone number, IP address, unique personal identifiers, online identifiers.
* **Commercial Information:** Records of products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.
* **Financial Information:** Payment card details (processed securely by third-party payment processors; we do not store full payment card numbers), billing address.
* **Account Information:** Username, password, preferences, feedback.
* **Communications:** Information you provide when contacting us, such as customer support inquiries, survey responses.
* **Professional or Employment-Related Information:** Job title, company name (if you interact with us in a business capacity).
* **Education Information:** (If relevant to our services, e.g., educational platforms).

#### 2.2. Usage Data

When you access our website, we may automatically collect certain information, including:

**Note**: This section is for data that is automatically collected. Update usage data below as appropriate.

* **Device Information:** IP address, browser type, browser version, operating system, unique device identifiers.
* **Usage Patterns:** Pages visited, time spent on pages, referral source, navigation paths, clickstream data.
* **Location Data:** General location derived from your IP address.
* **Cookies and Tracking Technologies:** Information collected through cookies, web beacons, and similar technologies (as detailed in our **[Link to Cookie Policy]**).

#### 2.3. Sensitive Personal Information

**Note**: This section outlines any special categories of data (examples may include health data, racial or ethnic origin, genetic data and other similar types of data). Revise the collection of sensitive personal information as appropriate.

**OPTION 1:**

**Note**: This option should be used by an organization when it has confirmed that it **does not** collect sensitive personal information.

We do not collect sensitive personal information (e.g., health data, racial or ethnic origin, political opinions, religious or philosophical beliefs, genetic data, biometric data, sexual orientation). If, for a specific service, we need to collect such data, we will clearly inform you, explain the purpose, and obtain your explicit consent or rely on another lawful basis as required by applicable global privacy laws.

*OR*

**OPTION 2:**

**Note**: This option should be used by an organization when it has confirmed that it currently collects sensitive personal information. All categories of data that are currently collected should be listed, as well as the instances when such data is collected. You should also list the safeguards that are in place by the organization to protect the sensitive personal information that is collected.

We may collect, use, store and otherwise process certain types of personal data that are considered sensitive, special category, or protected data, under global data protection laws. This may include, depending on your location and the services we provide:

**Note**: Remove categories of data as appropriate for your organization

* Racial or ethnic origin
* Political opinions
* Religious or philosophical beliefs
* Trade union membership
* Genetic or biometric data (used for identification)
* Physical or mental health data
* Sexual orientation or sex life
* Government-issued identifiers (e.g., social security, national ID numbers)
* Financial account information (where considered sensitive under applicable law)
* Precise geolocation data

We only process this type of data when:

* You have given your explicit consent, where required
* It is necessary to provide a service you have requested
* It is required or authorized by law
* It is necessary to protect your vital interests
* It is necessary for the establishment, exercise, or defense of legal claims
* It is in the substantial public interest, in line with applicable laws
* It is required for employment, social security, or social protection obligations

We implement appropriate safeguards to protect this information, including:

**Note**: Delete as applicable for your organization

* Encryption and secure storage
* Access restrictions and role-based controls
* Staff training and confidentiality obligations
* Data minimization and retention limits

We will never use sensitive personal data for marketing or profiling without your explicit consent where required.

Your rights regarding this data, including access, correction, deletion, objections, and withdrawal of consent, may vary depending on your jurisdiction. Please refer to the “7. Your Data Protection Rights” section of this policy or contact us at **[Insert contact email or alternative contact method]** for further details.

#### 2.4. Tracking Technologies

**Note**: Revise tracking technologies below as appropriate.

We and our third-party partners may use a variety of tracking technologies to collect information about your interactions with our website and services. These include:

* **Cookies:** Small text files stored on your device that help us remember your preferences, enable functionality, and analyze site usage. These are set by both our website (first-party cookies) and via our partners (third-party cookies).
* **Tracking Scripts / Analytics Tools:** Software (such as Google Analytics, Meta Pixel, Microsoft Clarity, or similar) that collects information about how you interact with our website.
* **Web Beacons / Pixels:** Tiny graphic images or scripts embedded in web pages or emails that track whether you have accessed certain content or opened an email.
* **Local Storage:** Technologies such as HTML5 local storage and browser cache, which store information locally on your device for faster access and improved experience.
* **Session Storage:** Temporary storage of data during your browser session, which is cleared when you close your browser.
* **Flash Cookies:** Also known as “local shared objects,” these can store preferences and activity data across sessions and browsers.
* **Device Fingerprinting**: Techniques that analyze information from your device, such as browser type, operating system, and settings, to uniquely identify your device.
* **Software Development Kits (SDKs):** Code embedded in our mobile applications to enable tracking across mobile devices.
* **Log Files:** Automatically recorded information about your device and usage upon each visit.

These technologies may be used for purposes such as enabling website functionality, remembering user preferences, providing analytics, enabling personalized content or ads, and maintaining the security of our services.

You may adjust your browser or device settings to limit or disable some tracking technologies, though certain features may not function properly without them.

## 3. How We Use Your Information

We use the collected data for various purposes, based on specific legal bases:

**Note**: A legal basis is required for processing personal data under GDPR and similar global privacy laws. This section shows how you adhere to laws around purpose limitation, lawfulness, fairness and transparency. If the Legal basis applies to your organization, the bullets below may be included:

* **To Provide and Maintain Our Service:** Including to process your transactions, manage your account, and deliver the services you request.

**Legal Basis**: Performance of a contract.

* **To Improve and Personalize Our Service:** To understand how you use our services, develop new features, and tailor content to your preferences.

**Legal Basis:** Legitimate interests (to improve our services) and/or consent. Where we rely on legitimate interests, we have conducted a balancing test to ensure our interests do not override your fundamental rights and freedoms. We obtain your consent through clear opt-in mechanisms, such as checkboxes that are not pre-ticked.

* **To Send You Marketing and Promotional Communications:** Where you have opted in about products, services, and offers that may be of interest to you.

**Legal Basis:** Consent. We obtain your consent through clear opt-in mechanisms, such as checkboxes that are not pre-ticked.

* **For Customer Support:** To respond to your inquiries, provide technical support, and resolve issues.

**Legal Basis:** Performance of a contract, legitimate interests (to provide good customer service).

* **For Analytics and Research:** To monitor and analyze trends, usage, and activities in connection with our services.

**Legal Basis:** Legitimate interests (to understand and improve our services) and/or consent (for non-essential cookies). Where we rely on legitimate interests, we have conducted a balancing test to ensure our interests do not override your fundamental rights and freedoms. We obtain your consent through clear opt-in mechanisms, such as checkboxes that are not pre-ticked.

* **For Security and Fraud Prevention:** To detect, prevent, and address technical issues, fraud, or illegal activities.

**Legal Basis:** Legitimate interests (to protect our business and users), legal obligation. Where we rely on legitimate interests, we have conducted a balancing test to ensure our interests do not override your fundamental rights and freedoms.

* **To Comply with Legal Obligations:** To meet our regulatory and legal requirements, such as tax and accounting obligations.

**Legal Basis:** Legal obligation.

* **For Advertising:** To deliver targeted advertisements to you (where you have opted in or as permitted by law).

**Legal Basis:** Consent (e.g., GDPR, CCPA opt-out preference signals). We obtain your consent through clear opt-in mechanisms, such as checkboxes that are not pre-ticked.

## 4. How We Share Your Information

We may share your personal data with third parties in certain circumstances, always ensuring appropriate safeguards are in place. Please refer to a list of our subprocessors, which may be found here **[insert link to subprocessors, if the entity has such a list; if not, provide a list herein this Policy]**.

**Note:** this section shows how and with whom your organization shares data collected.

4.1. Service Providers: We may engage third-party companies and individuals to facilitate our services, perform service-related services, or assist us in analyzing how our service is used (e.g., hosting providers, payment processors, analytics providers, email service providers). These third parties have access to your personal data only to perform these tasks on our behalf and are obligated not to disclose or use it for any other purpose.

4.2. Business Transfers: If **[Your Company Name]** is involved in a merger, acquisition, or asset sale, your personal data may be transferred. We will provide notice before your personal data is transferred and becomes subject to a different privacy policy.

4.3. Legal Requirements: We may disclose your personal data in the good faith belief that such action is necessary to:

* Comply with a legal obligation (e.g., subpoena or court order).
* Protect and defend the rights or property of **[Your Company Name]**.
* Prevent or investigate possible wrongdoing in connection with the service.
* Protect the personal safety of users of the service or the public.
* Protect against legal liability.

4.4. With Your Consent: We may disclose your personal data for any other purpose with your explicit consent.

4.5. Aggregated or De-identified Data: We may share aggregated or de-identified information that cannot reasonably be used to identify you.

## 5. International Data Transfers

**Note**: This section includes the specific safeguards your organization takes. Revise transfers of personal data below as appropriate.

Your information, including personal data, may be transferred to — and maintained on — servers located outside of your state, province, country, or other governmental jurisdiction where the data protection laws may differ from those of your jurisdiction.

For transfers of personal data from the European Economic Area (EEA), UK, or Switzerland to countries not deemed to provide an adequate level of data protection by the European Commission or relevant authorities, we implement appropriate safeguards, such as:

* **Standard Contractual Clauses (SCCs):** Approved by the European Commission, obliging recipients to protect personal data to the GDPR standards.
* **Binding Corporate Rules (BCRs):** For intra-group transfers, where applicable.
* **Data Transfer Agreements:** Ensuring equivalent protection as required by local laws (e.g., LGPD).

Where required, we conduct Transfer Impact Assessments to evaluate the level of protection in the recipient country and implement supplementary measures if necessary.

By providing your personal data, you consent to this transfer, storage, and processing. Where consent is the legal basis for transfer, you have the right to withdraw that consent at any time.

## 

## 6. Data Security and Retention

**Note**: This section outlines the security controls that your organization has in place to protect data, which are typically referred to as technical and organizational measures. Please revise the below listed technical and organizational security measures as appropriate.

6.1. Data Security: We employ industry-standard technical and organizational security measures to protect your personal data from unauthorized access, alteration, disclosure, or destruction. These measures include:

* **Encryption:** Using SSL/TLS encryption for data in transit (HTTPS).
* **Access Controls:** Restricting access to personal data to authorized personnel only.
* **Data Minimization:** Collecting only necessary data.
* **Regular Security Audits:** Conducting periodic reviews of our security practices.
* **Employee Training:** Educating our staff on data protection and security.
* **Pseudonymization/Anonymization:** Where feasible and appropriate.

While we strive to use commercially acceptable means to protect your personal data, no method of transmission over the internet or method of electronic storage is 100% secure. Therefore, we cannot guarantee its absolute security.

6.2. Data Retention: We will retain your personal data only for as long as is necessary for the purposes set out in this Policy, unless a longer retention period is required or permitted by law (e.g., for legal, tax, or accounting purposes).

When we no longer need your personal data, we will securely delete or anonymize it in accordance with applicable law.

## 7. Your Data Protection Rights

Depending on your location and applicable privacy laws, you have various rights regarding your personal data. We are committed to facilitating the exercise of these rights.

Note: This section outlines rights of data subjects under applicable global privacy laws to which your organization may be required to follow. Please revise data protection rights as appropriate.

#### 7.1. General Rights (Applicable Broadly, e.g., GDPR, CCPA, LGPD, PIPEDA, APPI, APPs):

* **Right to Be Informed:** You have the right to know what personal data we collect, why we collect it, and how we use it. This Policy serves to fulfill this right.
* **Right of Access:** You have the right to request a copy of the personal data we hold about you.
* **Right to Rectification (Correction):** You have the right to request that we correct any inaccurate or incomplete personal data we hold about you.
* **Right to Erasure (Deletion / “Right to Be Forgotten”):** You have the right to request the deletion of your personal data under certain circumstances (e.g., if the data is no longer necessary for the purposes for which it was collected).
* **Right to Restrict Processing:** You have the right to request that we restrict the processing of your personal data under certain conditions (e.g., if you contest the accuracy of the data).
* **Right to Data Portability:** You have the right to receive your personal data in a structured, commonly used, and machine-readable format and to transmit that data to another controller, where technically feasible.
* **Right to Object:** You have the right to object to the processing of your personal data based on legitimate interests or for direct marketing purposes.
* **Rights in Relation to Automated Decision-Making and Profiling:** You have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning you or similarly significantly affects you, unless certain exceptions apply.
* **Right to Withdraw Consent:** Where we rely on your consent to process your personal data, you have the right to withdraw that consent at any time. This will not affect the lawfulness of processing based on consent before its withdrawal.

#### 7.2. Specific Rights by Region:

* ***For California Residents (CCPA/CPRA):***
  + **Right to Know:** You have the right to request that we disclose the categories and specific pieces of personal information we have collected, the categories of sources from which personal information is collected, the business or commercial purpose for collecting, selling, or sharing personal information, and the categories of third parties to whom we disclose personal information.
  + **Right to Opt-Out of Sale or Sharing:** You have the right to opt-out of the “sale” or “sharing” of your personal information (as defined by CCPA/CPRA) for cross-context behavioral advertising. We provide a prominent “Do Not Sell or Share My Personal Information” link on our website footer.
  + **Right to Limit Use and Disclosure of Sensitive Personal Information:** You have the right to limit the use and disclosure of your sensitive personal information (as defined by CCPA/CPRA) to only that which is necessary to perform the services or provide the goods reasonably expected by an average consumer who requests those goods or services. We provide a prominent “Limit the Use of My Sensitive Personal Information” link on our website footer.
  + **Right to Non-Discrimination:** We will not discriminate against you for exercising any of your CCPA/CPRA rights.
  + **Right to Correct Inaccurate Personal Information.**
* ***For Brazilian Residents (LGPD):***
  + Similar rights to GDPR, including confirmation of processing, access, correction, anonymization/blocking/deletion, portability, deletion of data processed with consent, information about shared data, information about possibility of denying consent and consequences, and revocation of consent.
* ***For Canadian Residents (PIPEDA):***
  + Similar rights to access, correction, and challenging compliance. Emphasis on accountability, identifying purposes, consent, limiting collection, limiting use/disclosure/retention, accuracy, safeguards, openness, individual access, and recourse.
* ***For Japanese Residents (APPI):***
  + Similar rights to disclosure, correction, cessation of use, and deletion of personal information. Requirements for appropriate security measures and supervision of service providers.
* ***For Australian Residents (APPs):***
  + Similar rights to access and correction. Specific principles regarding collection, use, disclosure, data quality, data security, and direct marketing.
* ***For EU/UK Residents:***
  + If you believe your rights have been violated, you have the right to lodge a complaint with your local data protection authority. For the UK: <https://ico.org.uk/>; for the EU: <https://www.edpb.europa.eu/edpb_en>

7.3. How to Exercise Your Rights: To exercise any of these rights, please contact us at: **[Your DPO / Privacy Contact Email Address] [Link to your Data Subject Access Request (DSAR) Form, if applicable] [Your Company Phone Number]**

We will respond to your request within the timeframes required by applicable law (e.g., 30 days under GDPR, 45 days under CCPA). We may need to verify your identity before fulfilling your request. You may exercise your rights free of charge, unless requests are manifestly unfounded or excessive.

## 8. Children’s Privacy

**Note**: This section provides language related to services that are not aimed at children and the collection of children’s data. However, your organization may be aimed at children and require different language. Please revise as appropriate.

Our service is not intended for individuals under the age of [e.g., 16 for GDPR, 13 for COPPA]. We do not knowingly collect personally identifiable information from children without verifiable parental consent.

If you are a parent or guardian and you are aware that your child has provided us with personal data, please contact us. If we become aware that we have collected personal data from children without verification of parental consent, we take steps to remove that information from our servers.

## 9. Links to Other Websites

**Note**: Revise as appropriate.

Our services may contain links to other websites that are not operated by us. If you click on a third-party link, you will be directed to that third party’s site. We strongly advise you to review the privacy policy of every site you visit.

We have no control over and assume no responsibility for the content, privacy policies, or practices of any third-party sites or services.

## 10. Changes to This Privacy Policy

**Note:** This section outlines your organization’s updating of this policy from time-to-time. It is recommended under global privacy laws to review and update on an annual basis. However, please review the below language as appropriate.

We may update this Policy from time to time. We will notify you of any changes by posting the new Policy on this page and updating the “Last Updated” date at the top of this Policy.

We will also inform you via email and/or a prominent notice on our website prior to the change becoming effective, and update the “Effective Date.”

You are advised to review this Policy periodically for any changes. Changes to this Policy are effective when they are posted on this page.

## 11. Complaints and Supervisory Authorities

**Note:** This section outlines a website or service user’s rights to lodge a complaint with data protection supervisory authorities (if applicable to the user’s jurisdiction) and how to contact your organization with a complaint. Revise as appropriate.

If you have concerns about our privacy practices, please contact us directly using the details provided in Section 1 above.

You also have the right to lodge a complaint with the relevant data protection supervisory authority in your jurisdiction:

* ***For EU/EEA Residents:*** You can contact the data protection authority in your Member State. A list of authorities can be found here: [Link to European Data Protection Board (EDPB) list, if available, or instruct them to search for their local DPA].
* ***For UK Residents:*** Information Commissioner's Office (ICO)
* ***For Canadian Residents:*** Office of the Privacy Commissioner of Canada (OPC)
* ***For Brazilian Residents:*** Autoridade Nacional de Proteção de Dados (ANPD)
* ***For Australian Residents:*** Office of the Australian Information Commissioner (OAIC)
* ***For California Residents:*** California Attorney General or the California Privacy Protection Agency (CPPA).