Privacy Policy

Version: May 2026

About Us and This Policy

Ziflow Limited ("We") are committed to protecting and respecting your privacy.

This policy (together with our Terms of Service (if you are a customer) and any other documents referred to in this policy and in the Terms of Service) sets out the basis on which any personal data we collect from you, or that you provide to us, will be processed by us. Capitalised terms not defined in this Privacy Policy shall have the meaning given to them in:

1. our applicable Terms of Service (contained in the Online version of the Master Subscription Agreement)
2. in the General Data Protection Regulation (EU) 2016/679 (the "EU GDPR") or
3. the retained version of the EU GDPR in the UK as this has been established by European Union (Withdrawal) Act 2018 and amended by the Data (Use and Access) Act 2025 ("UK GDPR").

By visiting https://www.ziflow.com/ (our site) you are accepting and consenting to the practices described in this policy.

For the purpose of UK GDPR, the data controller is Ziflow Limited with its registered address at 1st Floor 48 Chancery Lane, London, England, WC2A 1JF. We are registered with the UK Information Commissioner's Office with registration reference number: ZA172378.

Ziflow is committed to protecting the security of your personal information and we take all reasonable precautions to protect it from unauthorised access, modification or disclosure. Your personal information is stored on secure servers that have SSL Certificates issued by leading certificate authorities, and all data transferred between you and the Service is encrypted. You can find out more about our security arrangements and our data protection measures on our security page.

Information We Collect About You

We will collect and process the following data about you:

Information you give us. This is information about you that you give us by filling in forms on our site or by corresponding with us by phone, e-mail or otherwise. It includes information you provide when you register to use our site, subscribe to our service, search for a product, place an order on our site, use social media functions on our site,

and when you report a problem with our site. The information you give us may include your name, address, e-mail address and phone number, financial and credit card information.

Information we collect. With regard to each of your visits to our site we will automatically collect the following information:

- technical information, including the Internet protocol (IP) address used to connect your computer to the Internet, your login information, browser type and version, time zone setting, browser plug-in types and versions;

- information about your visit, including your IP address, URL details, date and time of visit, products and pages you viewed or searched for, page response times, page interaction information (such as scrolling, clicks, and mouse-moves, methods used to browse away from the page, and any phone number used to call our customer service line.

Information we receive from other sources. This is information we receive about you from third parties. We are working closely with third parties (including, for example, business partners, sub-contractors in technical, payment and delivery services, advertising networks, analytics providers, search information providers, credit reference agencies).

Information Generated from AI Interactions. When you use our AI-powered features (e.g., project content, automated briefs, the features within ReviewAI), we collect the text prompts, inputs, and feedback you provide (such as “good” and “bad” ratings).

- **Usage:** This data is used solely to generate the immediate response and to calculate internal accuracy scores.
- **No Model Training:** We do **not** use your data to train, retrain, or improve the third-party AI models that power these features. We currently avail of a range of large language models on a non-exclusive basis and reserve the right to remain flexible and interchange given the pace of progress in the AI and augmented reasoning, proofing and review sectors. Currently we use OpenAI and Google Gemini among others and can provide assurance that your inputs remain isolated to your instance and your use-case only.

Sensitive Data. This is personal data such as biometric data for unique identification, health information and medical records, racial or ethnic origin, political orientation or beliefs, religious or philosophical beliefs, trade union membership, data concerning sex

life or sexual orientation, genetic data. We do not collect any sensitive personal data and we do not want you to give us sensitive data.

Information about other individuals. If you give us information on behalf of someone else, you confirm that the other person has appointed you to act on his/her behalf and has agreed that you can:

- give consent on his/her behalf to the processing of his/her personal data;
- receive on his/her behalf any data protection notices; and
- give consent to the transfer of his/her personal as contemplated in this privacy policy.

Cookies

We use the following cookies:
• **Essential:** These are cookies that are required for the operation of our website. They include, for example, cookies that enable you to log into secure areas of our website, use a shopping cart or make use of e-billing services.
• **Analytical:** These allow us to recognise and count the number of visitors and to see how visitors move around our website when they are using it. This helps us to improve the way our website works, for example, by ensuring that users are finding what they are looking for easily.
• **Functional:** These are used to recognise you when you return to our website. This enables us to personalise our content for you, greet you by name and remember your preferences (for example, your choice of language or region).
• **Advertisement/Targeting:** These cookies record your visit to our website, the pages you have visited and the links you have followed. We will use this information to make our website and the advertising displayed on it more relevant to your interests. We may also share this information with third parties for this purpose.

Most browsers are set up to accept cookies automatically. But you can deactivate the storage of cookies or set your browser to notify you as soon as cookies are used and you can refuse the storage of cookies.

For detailed information on the cookies we use and the purposes for which we use them see our Cookie Policy.

Our Lawful Bases for Making Use of Your Personal Information

We use information held about you in the following ways:

Information we receive from other sources. We will combine the information we receive from the third parties that we are working with, with information you give to us and information we collect about you. We will use this information and the combined

information for the purposes set out above (depending on the types of information we receive).

Marketing and Opting Out

We do use your data to provide you, or permit selected third parties to provide you, with information about products or services we feel may interest you. If you are an existing customer, we will only contact you by electronic means (e.g. email) with information about goods and services similar to those which were the subject of a previous sale or negotiations of a sale to you. If you are a new customer, and where we permit selected third parties to use your data, we (or they) will contact you by electronic means only if you have consented to this or where we have established that it is in our legitimate interests to do so and this does not prejudice your rights.

Our Lawful Bases for Processing Your Data

There are six potential lawful bases for processing data under current law. We at Ziflow rely on no fewer than three of these bases for all of our work and processing.

Our primary lawful purposes are the following:

User Type/ Processing Activity	Data Categories Collected	Primary Purpose of Processing	Lawful Basis
Website Visitor			
Website Operation & Personalisation	Technical and usage data (including online identifies, IP address, device type, browser settings, log-in records).	For security, administration, fraud, monitoring and enhancing user experience.	Legitimate interest and consent, through our terms of service and accepting cookies.
Submissions, enquiries about	Identity and contact	To provide updates, record marketing	Consent (for marketing),

Ziflow products including ReviewAI	information (including name, email), marketing data (preferences, feedback, survey responses) or account information for support requests.	preferences, respond to support queries, improve user experience of our products and update our processes.	legitimate interest and legal obligation.
If you are a registered End-User of our Services, Platform and Products			
Core Service Provision	Transaction history, usage data, identity and contact data.	To provide products and services to Ziflow users	Contractual necessity (performance of Services)
Data Enrichment &Uploads	Enhanced data and prompts given to us when you use the products (such as ReviewAI)	Generating our results and insights plus personalisation.	Legitimate interests.
Payment facilitation	Payment data (with our payment partner)	To execute payments for the Ziflow products and services	Contractual Necessity
Customer services, customer comms, suggestions and feedback services	Emails, forms, opinions, user experiences	To continually improve the products, update the product information or terms of service and avoid complaints and risks using	Legitimate Interests

		great comms teams	

Opting out, Objecting and Unsubscribing

Please note you have a right to object and to seek to restrict direct marketing which comes from us or on our behalf. See the 'Your Rights' section for more information on how to exercise your right to object.

We will consider several factors when assessing an objection including: our users' reasonable expectations; the benefits and risks to you, us, other users, or third parties; and other available means to achieve the same purpose that may be less invasive and do not require disproportional effort. If your objection is upheld, we will cease processing your information, unless the processing is based on compelling legitimate grounds or is needed for legal reasons.

Where you have given your permission and you change your mind and you no longer wish to receive marketing and promotional communications from us, you may unsubscribe or opt-out of receiving them by following the instructions included in each newsletter or communication or by contacting us. See the 'Contact' section below.

We will also offer you the opportunity to choose (opt-out) whether your personal data is (a) to be disclosed to a third party, or (b) to be used for a purpose other than the purpose for which it was originally collected or subsequently authorized by you.

See further 'Your Rights', below for more information about what you can do in relation to your personal data collected and used by us.

Disclosure of Your Information

You agree that we have the right to share your personal information with:

- Selected third parties including:
  - business partners (such as resellers of our products and services), service providers, suppliers, agents and sub-contractors for the performance of any contract we enter into with them or you;
  - analytics and search engine providers that assist us in the improvement and optimisation of our site (see our Cookie Policy for more information on analytics cookies);
  - card payment service providers to process payments made by you using a credit or debit card.

We will disclose your personal information to third parties:

- In the event that we sell or buy any business or assets, in which case we will disclose your personal data to the prospective seller or buyer of such business or assets.
- If Ziflow Limited or substantially all of its assets are acquired by a third party, in which case personal data held by it about its customers will be one of the transferred assets.
- If we are under a duty to disclose or share your personal data in order to comply with any legal obligation, or in order to enforce or apply our Terms of Service or any other terms and conditions of supply or other contract we have entered into with you; or to protect the rights, property, or safety of Ziflow Limited, our customers, or others. This includes exchanging information with other companies and organisations for the purposes of fraud protection and credit risk reduction.

For a summary list of current but non-exhaustive third-party subprocessors we use, please note the current list maintained in our security trust center and available here, https://trust.ziflow.com/subprocessors

Data Storage and International Transfers

By submitting your personal data to us, you agree to the transfer, storing and processing of your data by us or on our behalf. Wherever we are required to transfer your personal information, regardless of where this occurs, we always take steps to ensure that your information is treated securely and in accordance with this privacy policy and all applicable data protection laws and regulations. We have noted the

maturing practices surrounding data transfer risk assessments and remain ready to conduct a bespoke transfer risk assessment should any change in opportunity, circumstance, or our geographical footprint change

We store and process "client" data in a few different ways:

1. US data center customers – we store their data in the US data center which comprises data such as comments, proofs, files, assets, and contacts;
2. EU data center customers – we store their data in our new EU data center which also comprises the same data sets (but not the same data), including comments, proofs, files, assets and contacts.
3. The "shared" component which spans regions and different territories relates to users and tenants. This data will be more centrally held in the United States although a degree of record-replication will occur across our different regions to ensure localised knowledge, control and quality of service. This kind of record-replication is required for affects global login functionality, activity logging, billing processes and operations, and invoice generation.

Wherever personal data sets are held, individuals can be assured that if we transfer personal data outside the EU and USA, for example from one of these locations to the other, we ensure that the transfer complies with applicable law by implementing appropriate safeguards.

i. For EU to US - Using the EU Standard Contractual Clauses (SCCs) plus transfer impact assessments or the EU to US Data Privacy Framework if available (approved by the European Commission in 2023)
ii. For US to EU or US to UK- using good quality data processing agreements
iii. For UK to US – using the UK to US Data Bridge which builds on the Data Privacy Framework or using the tailored addendum to the SCCs (or the standalone UK International Data Transfer Addendum (IDTA);
iv. Other territories - Transferring data to countries recognised as providing an adequate level of data protection by the UK Government and European Commission ideally or using alternate data transfer mechanisms..

We Do Not Store Your Credit Card Data

If you choose to pay for the service by credit card, your credit card details are not stored by the Service and cannot be accessed by Ziflow staff. Your credit card details are encrypted and securely stored by our sub-processor Chargify to enable Ziflow to

automatically bill your credit card on a recurring basis. You should review Chargify's Privacy Policy to ensure you are happy with it.

Data Security

Ziflow is committed to protecting the confidentiality, integrity and accuracy of your personal data. Our security framework is subject to independent assurance and regulatory standards and includes the following key tools and components:

1. Ziflow is ISO 27001:2022 certified, demonstrating our commitment to maintaining a robust Information Security Management System (ISMS) and Data Protection Management System (DPMS). Ziflow is also SOC 2 Type 2 certified as well, which is an important accreditation for Saas and managed service provider solutions to show they are protecting customer and partner data to a high standard. These certifications underpin our compliance under Article 32 of the UK GDPR, governing the security of our processing, ensuring a comprehensive, risk-based approach to data protection.
2. Internal controls and disciplines contained in the Company's AI/ML Governance Policy where team members are trained in the correct and safest way to deploy artificial intelligence and machine learning in all that we do.
3. Data Protection Impact Assessments (DPIAs) - We proactively manage risk at Board level. We are aware of our rights to conduct Data Protection Impact Assessments (DPIAs) prior to commencing any new product such as Review AI, deploying any new technology, or launching any new major facility or resource in for example Europe – especially if these may be considered to pose some element of risk to the rights and freedoms of individuals.
4. Data Breach Preparedness - Protocols - In the event of a personal data breach, Ziflow maintains an appropriate incident response plan. We follow a risk-based approach to breach notification in accordance with ICO guidance:
    i. We notify the Information Commissioner's Office (ICO) of any personal data breach that is likely to result in a risk to your rights and freedoms without undue delay and, where feasible, within 72 hours after becoming aware of the breach.
    ii. If a breach is likely to result in a high risk to your rights and freedoms, we will notify you directly and without undue delay so you can take protective measures.

5. Other technical and organisational measures - password and username controls that are unique to you;
    i. we run diagnostics and penetration testing exercises regularly;
    ii. we store your personal data on secure servers;
    iii. we use and review data processing agreements for our key 3rd party relationships
    iv. no credit card data is stored by us.

Where we have given you (or where you have chosen) a password which enables you to access certain parts of our site, you are responsible for keeping this password confidential. **We ask you not to share a password with anyone.**

Unfortunately, the transmission of information via the internet is not completely secure. Although we will do our best to protect your personal data, we cannot guarantee the security of your data transmitted to our site; any transmission is at your own risk. Once we have received your information, we will use strict procedures and security features to try to prevent unauthorised access.

Protection of Personal Data and Approach to Anonymised Data

Post-Retention Anonymisation: Data that is no longer necessary for regulatory or contractual purposes, but is valuable for refining our products or applications or our AI enabled tools, will be subject to robust, irreversible anonymisation techniques. Once irreversibly anonymised, this data no longer constitutes personal data under the UK GDPR and may be retained indefinitely for statistical and research purposes.

Pseudonymisation: We note that pseudonymised data remains personal data because, as long as the controller retains the key to re-identify the individual, it is subject to the same retention limitations as fully identifiable data.

How Long We Keep Your Data

We only keep your information for so long as it is necessary to fulfill the purpose for which it was collected.

We use the following criteria to determine whether or not we need to keep your data:

- fulfillment of an order,
- if you or we close your customer account,

- if you unsubscribe from direct marketing, newsletter or other material which we send to you,
- if we are required to keep a copy of your data by law or statutory regulation.

You also have the ability to request that we delete your personal data at any time. See the section below on 'Your Rights'.

Information that is archived is anonymised and kept for statistical analysis and research purposes.

Your Rights

Right to ask us to stop contacting you with direct marketing. Even if you have accepted the processing of your personal data for marketing purposes (by ticking the relevant box), you have the right to ask us to stop processing your personal data for such purposes. Let us know what method of contact you are not happy with if you are unhappy with certain ways of contacting you only (for example, you may be happy for us to contact you by email but not by telephone).

Right to request a copy of your information. You can request a copy of your information which we hold (this is known as a subject access request). If you would like a copy of some or it, please contact us and let us know the information you want a copy of, including any account or reference numbers, if you have them. Any subject access request may be subject to a reasonable fee to cover the cost of providing you with details of the information we hold about you.

Right to correct any mistakes in your information. You can require us to correct any mistakes in your information which we hold free of charge. If you would like to do this, please contact us and let us know the information that is incorrect and the information you want it replaced with.

Right to request we cease processing your information. You may request that we cease processing your personal data. If you make such a request, we shall retain only the amount of personal data pertaining you that is necessary to ensure that no further processing of your personal data takes place.

Right to request deletion of your information. You can ask us to erase all your personal data (also known as the "right to be forgotten") in the following circumstances:

- it is no longer necessary for us to hold that personal data with respect to the purpose for which it was originally collected or processed;
- you wish to withdraw your consent to us holding and processing your personal data;

- you object to us holding and processing your personal data (and there is no overriding legitimate interest to allow us to continue doing so);
- the personal data has been processed unlawfully; or
- the personal data needs to be erased in order for us to comply with a particular legal obligation.

Unless we have reasonable grounds to refuse to erase your personal data, all requests for erasure shall be complied with.

Changes to Our Policy

Any changes we make to our privacy policy in the future will be notified to you. Please check back frequently to see any updates or changes to our privacy policy.

Contact

Ziflow is not obliged to have a dedicated Data Protection Officer in post, but nevertheless questions, comments and requests regarding this privacy policy are welcomed and should be addressed to support@ziflow.com or by filling out the form on our Contact page. Please use these contact details to exercise your rights as outlined in the 'Your Rights' section above.

Complaints

If you have any complaints about the way in which we collect, store and use your information, Please write to us first, where we will strive to resolve the issue in every case. Only where these have not been addressed by contacting us first, you can contact the supervisory authority in the United Kingdom, the Information Commissioner's Office: https://ico.org.uk/concerns/

Links to Other Websites

Our website may contain links to other websites of interest. However, once you have used these links to leave our site, you should note that we do not have any control over other websites and their content. Therefore, we cannot be responsible for the protection and privacy of any information which you provide whilst visiting such sites and such sites are not governed by this privacy statement. You should exercise caution and look at the privacy statement applicable to the website in question.