

PRIVACY POLICY

Welcome to Send Files, a service provided by Publishd PTY LTD ("we," "us," or "our"). This Privacy Policy describes how we collect, use, and handle your personal information and data in a manner consistent with privacy laws, including the Australian Privacy Principles (APPs), the General Data Protection Regulation (GDPR), and the California Consumer Privacy Act (CCPA).

1. We respect your privacy

- (a) Publishd PTY LTD respects your right to privacy and is committed to safeguarding the privacy of our customers and website visitors. This policy sets out how we collect and treat your personal information.
- (b) We adhere to the Australian Privacy Principles contained in the *Privacy Act 1988* (Cth) and to the extent applicable, the EU General Data Protection Regulation (GDPR).
- (c) "Personal information" is information we hold which is identifiable as being about you. This includes information such as your name, email address, identification number, or any other type of information that can reasonably identify an individual, either directly or indirectly.
- (d) You may contact us in writing at 1/1 Midway Drive, New South Wales, 2035 for further information about this Privacy Policy.

2. What personal information is collected

- (a) Publishd PTY LTD will, from time to time, receive and store personal information you submit to our website, provided to us directly or given to us in other forms.
- (b) You may provide basic information such as your name, address and email address to enable us to send you information, provide updates and process your product or service order.
- (c) We may also collect
 - (i) Account & billing: email, name, plan, App IDs, billing status
 - (ii) Login & storage account: SFTP username, server URL, session/API tokens, linked Memberstack account
 - (iii) Your content: uploaded files, paths, filenames, embedded IPTC/XMP metadata
 - (iv) Auto Caption (optional): person names, reference face images, recognition results, captions, biometric face data processed via AWS Rekognition
 - (v) Sync (optional): destination settings, encrypted third-party credentials, sync logs

- (vi) Shares (optional): share settings, file lists, optional share passwords, recipient access events
- (vii) Configuration: rename rules, metadata/caption templates, feature settings
- (viii) Technical data: IP address, browser/device info, usage and error logs
- (d) We may collect additional information at other times, including but not limited to, when you provide feedback, when you provide information about your personal or business affairs, change your content or email preference, respond to surveys and/or promotions, provide financial or credit card information, or communicate with our customer support.
- (e) Additionally, we may also collect any other information you provide while interacting with us.

3. How we collect your personal information

- (a) Publishd PTY LTD collects personal information from you in a variety of ways, including when you interact with us electronically or in person, when you access our website and when we engage in business activities with you. We may receive personal information from third parties. If we do, we will protect it as set out in this Privacy Policy.
- (b) By providing us with personal information, you consent to the supply of that information subject to the terms of this Privacy Policy.

4. How we use your personal information

- (a) Publishd PTY LTD may use personal information collected from you to provide you with information about our products or services. We may also make you aware of new and additional products, services and opportunities available to you.
- (b) Publishd PTY LTD will use personal information only for the purposes that you consent to. This may include to:
 - (i) provide you with products and services during the usual course of our business activities;
 - (ii) administer our business activities;
 - (iii) manage, research and develop our products and services;
 - (iv) provide you with information about our products and services;
 - (v) communicate with you by a variety of measures including, but not limited to, by telephone, email, sms or mail; and
 - (vi) investigate any complaints.

If you withhold your personal information, it may not be possible for us to provide you with our products and services or for you to fully access our website.

We retain personal information for up to 30 days after our business relationship ends or last service interaction, after which it will be securely deleted or anonymized unless

legally required to retain it longer. You may request earlier deletion of your data by contacting our Data Protection Officer.

- (c) We may disclose your personal information to comply with a legal requirement, such as a law, regulation, court order, subpoena, warrant, legal proceedings or in response to a law enforcement agency request.
- (d) If there is a change of control in our business or a sale or transfer of business assets, we reserve the right to transfer to the extent permissible at law our user databases, together with any personal information and non-personal information contained in those databases.

5. Sub-Processors

- (a) As a Data Processor, Publishd PTY LTD engages the following third-party sub-processors to assist in delivering the Send Files platform and its associated services. Each sub-processor is bound by data processing agreements that impose equivalent data protection obligations to those set out in this Privacy Policy, in accordance with GDPR Article 28, Australian Privacy Principle 8, and the CCPA. We will notify users of any material changes to our sub-processor list by updating this policy and, where required, seeking fresh consent.
- (b) **Current Sub-Processors** - The following sub-processors are currently engaged by Publishd PTY LTD in connection with the operation of the Send Files platform:
 - (i) **Vultr** — Country of Processing: Global (multiple regions); Purpose: Hosting of SFTP nodes for secure file transfer; Data Processed: Uploaded files, file paths, filenames, and associated metadata; Safeguards: Data Processing Agreement (DPA), encryption in transit via SSH/SFTP, and encryption at rest.
 - (ii) **Netcup** — Country of Processing: United States; Purpose: Processing for sync transfers between storage destinations; Data Processed: File content, destination settings, sync logs, and encrypted third-party credentials; Safeguards: Data Processing Agreement (DPA), Standard Contractual Clauses (SCCs) as approved by the European Commission, and encryption in transit.
 - (iii) **Hetzner** — Country of Processing: Germany (European Economic Area); Purpose: Thumbnail generation from uploaded images; Data Processed: Uploaded images and associated file metadata; Safeguards: Data Processing Agreement (DPA). As Germany is a member of the EEA, transfers are not restricted under the GDPR.
 - (iv) **Cloudflare** — Country of Processing: Global (multiple regions); Purpose: Compute processing, credential storage, and content delivery; Data Processed: Account credentials (encrypted), session tokens, API tokens, and technical usage data; Safeguards: Data Processing Agreement (DPA), Standard Contractual

Clauses (SCCs), AES-256-GCM encryption for stored credentials, and Cloudflare's binding corporate rules.

- (v) **Memberstack** — Country of Processing: United States; Purpose: Membership management and user authentication; Data Processed: Account details including email address, plan information, and membership status; Safeguards: Data Processing Agreement (DPA) and Standard Contractual Clauses (SCCs) as approved by the European Commission.
- (vi) **Webflow** — Country of Processing: United States; Purpose: Frontend website hosting and content management; Data Processed: Website usage data, browser and device information, and IP addresses; Safeguards: Data Processing Agreement (DPA) and Standard Contractual Clauses (SCCs) as approved by the European Commission.
- (vii) **Stripe** — Country of Processing: United States; Purpose: Payment processing and billing management; Data Processed: Payment card details, billing information, transaction records, and billing status; Safeguards: Data Processing Agreement (DPA), Standard Contractual Clauses (SCCs), PCI-DSS Level 1 compliance, and end-to-end encryption of payment data. Stripe does not store full card details on our behalf.
- (viii) **Google (Gmail)** — Country of Processing: United States; Purpose: Email hosting, initial account provisioning, and customer support ticket management; Data Processed: Email addresses, account correspondence, and support ticket content; Safeguards: Data Processing Agreement (DPA), Standard Contractual Clauses (SCCs), and Google Workspace security certifications including ISO 27001.
- (ix) **Make.com** — Country of Processing: European Union; Purpose: Workflow automations involved in user account creation and updates; Data Processed: Account details, email addresses, plan information, and user status updates; Safeguards: Data Processing Agreement (DPA) and Standard Contractual Clauses (SCCs) as approved by the European Commission.
- (x) **Backblaze** — Country of Processing: United States and the Netherlands (European Economic Area); Purpose: Cloud file storage for uploaded user files; Data Processed: Uploaded files, file paths, filenames, and associated metadata; Safeguards: Data Processing Agreement (DPA), Standard Contractual Clauses (SCCs) as approved by the European Commission for transfers to the United States bucket, and encryption in transit and at rest. Transfers to the Amsterdam bucket are not restricted under the GDPR as the Netherlands is a member of the EEA. All stored data is encrypted using AES-256 encryption at rest.

- (xi) **Amazon Web Services (AWS)** — Country of Processing: Australia (and other AWS regions as applicable); Purpose: (1) Transactional and marketing email delivery via Amazon SES; and (2) AI image processing and facial recognition for the Auto-Caption feature via AWS Rekognition; Data Processed: Email addresses and email content (SES); uploaded images, facial vectors, biometric data, person names, and recognition results (Rekognition); Safeguards: Data Processing Agreement (DPA), Standard Contractual Clauses (SCCs), AWS ISO 27001 and SOC 2 certifications, encryption in transit and at rest, and AWS's binding corporate rules. As AWS processes biometric data on our behalf, it is subject to the additional safeguards described in clause 6 of this Privacy Policy.

Changes to Sub-Processors

- 5.1. We will provide at least 30 days' prior written notice of any intended addition or replacement of sub-processors by updating this Privacy Policy and notifying users via email where required. If you object to the engagement of a new sub-processor on legitimate grounds relating to the protection of your personal data, please contact our Data Protection Officer at support@send-files.com within 14 days of receiving notice. We will work with you in good faith to address your concerns, and where we are unable to do so, you may terminate your account in accordance with our Terms of Service.
- 5.2. **Overseas Disclosure — Australian Privacy Principle 8** - In accordance with Australian Privacy Principle 8, we disclose that personal information may be transferred to and processed by sub-processors located overseas, including in the United States, Germany, and the European Union. Before disclosing personal information to an overseas recipient, we take reasonable steps to ensure that the recipient does not breach the Australian Privacy Principles in relation to that information. Where we are unable to ensure equivalent protection, we will seek your consent to the overseas disclosure or rely on an applicable exception under the Privacy Act 1988 (Cth).

6. Disclosure of your personal information

- (a) Publishd PTY LTD may disclose your personal information to any of our employees, officers, insurers, professional advisers, agents, suppliers or subcontractors insofar as reasonably necessary for the purposes set out in this privacy policy.
- (b) If we do disclose your personal information to a third party, we will protect it in accordance with this privacy policy.
- (c) Artificial Intelligence and Biometric Data Processing

- (a) **Overview of AI Functionality** - Our website and application utilise artificial intelligence (AI) technology, hosted on Amazon Web Services (AWS), to assist editorial photographers and other users in identifying and captioning individuals appearing in uploaded images. This functionality involves the collection and processing of biometric data, which is classified as sensitive personal information under the Privacy Act 1988 (Cth) and as special category data under the GDPR.
- (b) **Biometric Data We Collect** - To facilitate the AI-powered image captioning and facial recognition functionality, we collect and process the following categories of data as a Data Processor on behalf of our users:
 - (i) images uploaded by users to our platform;
 - (ii) user-added names and identifying information associated with individuals appearing in those images;
 - (iii) facial vectors — mathematical representations derived from facial geometry that enable the system to identify and match faces across multiple images; and
 - (iv) any associated metadata generated during the image processing workflow.
- (c) **Legal Basis for Processing Biometric Data** - The collection and processing of biometric data, including facial vectors, constitutes the handling of sensitive personal information. We will only collect and process such data where:
 - (i) we have obtained the explicit consent of the individual whose biometric data is being processed, or the user uploading the content has confirmed they hold the appropriate authority or consent to do so;
 - (ii) processing is necessary for the legitimate purposes of editorial, journalistic, or commercial photography in accordance with applicable law; or
 - (iii) processing is otherwise permitted under the Privacy Act 1988 (Cth), the Australian Privacy Principles, or the GDPR (including Article 9(2)) as applicable.
- (d) **Our Role as Data Processor** - Where users upload images containing personal or biometric data of third parties, Publishd PTY LTD acts as a Data Processor on behalf of the user (who is the Data Controller). Users are responsible for ensuring they have obtained all necessary consents and legal authority to upload and process images containing identifiable individuals, including any biometric data. By uploading such content, users warrant that they have complied with all applicable privacy laws and obtained any required consents from the individuals depicted.
- (e) **AWS as a Sub-Processor** - We engage Amazon Web Services (AWS) as a sub-processor to provide cloud infrastructure and AI image processing services, including facial recognition capabilities. AWS processes biometric and personal data solely on our instructions and in accordance with our data processing agreement with AWS. AWS maintains appropriate technical and organisational security measures and complies with

applicable data protection laws, including the GDPR. Details of AWS's data processing and security practices are available at <https://aws.amazon.com/privacy/>. By using our platform, you acknowledge and consent to the transfer and processing of your data by AWS in accordance with this Privacy Policy.

- (f) **Retention of Biometric Data** - Facial vectors and other biometric data are retained only for as long as is necessary to provide the AI captioning functionality and for no longer than the period during which the associated user account remains active. Upon account deletion or upon a user's request, all facial vectors and associated biometric data will be permanently deleted from our systems and from AWS infrastructure within 30 days, unless we are required by law to retain such data for a longer period. Raw images may be retained in accordance with our general data retention policy set out in clause 4(b) above.
- (g) **Rights in Relation to Biometric Data** - Individuals whose biometric data has been processed through our platform have the right to:
- (i) request access to any biometric data held about them;
 - (ii) request the deletion of their facial vectors and associated biometric data;
 - (iii) withdraw consent to the processing of their biometric data at any time, without affecting the lawfulness of processing carried out prior to withdrawal; and
 - (iv) object to automated processing and profiling based on their biometric data.
- (h) To exercise any of these rights, please contact our Data Protection Officer at support@send-files.com. We will respond to all requests within 30 days in accordance with our obligations under the Privacy Act 1988 (Cth) and the GDPR.
- (i) **Data Retention Schedule** - We maintain the following retention periods for personal data processed through our platform:
- (i) photographer registration and portfolio data is retained while the account remains active and deleted within 30 days of account deletion;
 - (ii) client project data is retained for the duration of the engagement plus 2 years for dispute resolution purposes, after which it is permanently deleted;
 - (iii) biometric data including facial vectors is deleted within 30 days of account deletion or upon request;
 - (iv) transaction and financial records are retained for 7 years in accordance with Australian taxation requirements under the Income Tax Assessment Act 1997 (Cth); and
 - (v) all other personal data is deleted within 30 days of the end of our business relationship or last service interaction. Users may request early deletion of their data by contacting our Data Protection Officer, and we will action such requests within 30 days unless retention is required by law.

- (j) **Photographer Consent Verification** - Users uploading images or project data containing identifiable individuals confirm at the time of upload that they hold all necessary consents from clients and depicted individuals, and have complied with applicable privacy laws in their jurisdiction. We reserve the right to request evidence of consent, including client agreements or model releases, if a complaint or challenge arises. Users warrant their compliance with all applicable privacy obligations. Where a user uploads content without holding the requisite consents, that user shall be solely responsible for any resulting claims, regulatory action, or losses. Publishd PTY LTD's liability in such circumstances is limited to the extent permitted by law, and nothing in this clause limits any rights you may have under the Australian Consumer Law or applicable data protection legislation.
 - (k) **Children and Biometric Data** - We do not knowingly collect or process biometric data of individuals under the age of 16 without the explicit consent of a parent or legal guardian. Users must not upload images containing identifiable children for AI processing without first obtaining the required parental or guardian consent. If we become aware that biometric data of a child has been collected without appropriate consent, we will delete such data immediately.
 - (l) **Data Protection Impact Assessment** - Given the nature of biometric data processing and the use of facial recognition technology, Publishd PTY LTD has conducted and will maintain a Data Protection Impact Assessment (DPIA) in accordance with Article 35 of the GDPR. This assessment evaluates the risks associated with our AI processing activities and the measures we have implemented to mitigate those risks. A summary of our DPIA is available upon request by contacting our Data Protection Officer
- (d) Australian Privacy Principles (APPs)
- (a) **APP 1 — Open and Transparent Management** - Publishd PTY LTD is committed to managing personal information in an open and transparent way. This Privacy Policy sets out how we collect, hold, use, and disclose personal information in accordance with the Australian Privacy Principles contained in the Privacy Act 1988 (Cth). A copy of this Privacy Policy is available free of charge upon request by downloading directly from this web page.
 - (b) **APP 3 — Collection of Solicited Personal Information** - We only collect personal information that is reasonably necessary for, or directly related to, one or more of our functions or activities. Where it is reasonable and practicable to do so, we will collect personal information directly from you. We will not collect sensitive information about you without your consent, unless an exception under the APPs applies.
 - (c) **APP 5 — Notification of Collection** - At or before the time we collect personal information about you, or as soon as practicable afterwards, we will take reasonable steps to notify you of:

- (i) our identity and contact details;
 - (ii) the purposes for which we are collecting the information;
 - (iii) the main consequences if the information is not collected; and
 - (iv) any other entities to whom we usually disclose information of that kind.
 - (d) **APP 6 — Use and Disclosure** - We will only use or disclose personal information for the primary purpose for which it was collected, or for a secondary purpose if you have consented to that use or disclosure, or if an exception under the APPs applies. We will not use or disclose personal information for the purpose of direct marketing unless you have consented to receive such communications, and we will always provide you with a simple means to opt out.
 - (e) **APP 11 — Security of Personal Information** - We take reasonable steps to protect personal information we hold from misuse, interference, loss, and from unauthorised access, modification, or disclosure. Where we no longer require personal information for any purpose for which it may be used or disclosed under the APPs, and we are not required by law to retain it, we will take reasonable steps to destroy or de-identify that information.
 - (f) **APP 12 — Access and Correction** - You have the right to request access to personal information we hold about you, and to request that we correct that information if it is inaccurate, out of date, incomplete, irrelevant, or misleading. To make such a request, please contact us at support@send-files.com. We will respond to your request within a reasonable period and, where reasonable and practicable, provide access in the manner you request.
- (e) California Consumer Privacy Act (CCPA)
- (a) **Applicability** - This section applies to individuals who are residents of the State of California, United States. To the extent that the California Consumer Privacy Act 2018 (CCPA), as amended by the California Privacy Rights Act 2020 (CPRA), applies to our processing of your personal information, we provide the following additional disclosures.
 - (b) **Categories of Personal Information Collected** - In the preceding 12 months, we have collected the following categories of personal information from California residents:
 - (i) identifiers such as name, email address, and IP address;
 - (ii) commercial information, including records of products or services purchased;
 - (iii) internet or other electronic network activity information, including browsing history and interactions with our website; and
 - (iv) biometric information, including facial vectors derived from images uploaded to our platform.
 - (c) **Your Rights Under the CCPA** - If you are a California resident, you have the following rights in relation to your personal information:

- (i) **Right to Know** — you have the right to request that we disclose the categories and specific pieces of personal information we have collected about you, the categories of sources from which it was collected, the purposes for collection, and the categories of third parties with whom we share it;
 - (ii) **Right to Correct** — you have the right to request that we correct inaccurate personal information we hold about you;
 - (iii) **Right to Delete** — you have the right to request the deletion of personal information we have collected from you, subject to certain exceptions;
 - (iv) **Right to Opt-Out of Sale or Sharing** — we do not sell your personal information to third parties, nor do we share your personal information for cross-context behavioural advertising purposes; and
 - (v) **Right to Non-Discrimination** — we will not discriminate against you for exercising any of your rights under the CCPA, including by denying you goods or services, charging different prices, or providing a different level of service.
- (d) **How to Exercise Your CCPA Rights** - To exercise any of your rights under the CCPA, please submit a verifiable consumer request to us by emailing support@send-files.com. We will respond to your request within 45 days of receipt. If we require more time, we will notify you of the reason and the extension period in writing. We may ask you to verify your identity before processing your request.
- (e) **Authorised Agents** - You may designate an authorised agent to submit a CCPA request on your behalf. To do so, you must provide the authorised agent with written permission to act on your behalf, and we may require you to verify your identity directly with us before processing the request.
- (f) **General Data Protection Regulation (GDPR) for the European Union (EU)**
 - (a) Publishd PTY LTD will comply with the principles of data protection set out in the GDPR for the purpose of fairness, transparency and lawful data collection and use.
 - (b) We process your personal information as a Processor and/or to the extent that we are a Controller as defined in the GDPR.
 - (c) We must establish a lawful basis for processing your personal information. The legal basis for which we collect your personal information depends on the data that we collect and how we use it.
 - (d) We will only collect your personal information with your express consent for a specific purpose and any data collected will be to the extent necessary and not excessive for its purpose. We will keep your data safe and secure.
 - (e) We will also process your personal information if it is necessary for our legitimate interests, or to fulfil a contractual or legal obligation.

- (f) Where we rely on legitimate interests as a lawful basis, we conduct a balancing test to ensure our processing does not infringe your rights and freedoms. Our legitimate interests include improving our services, preventing fraud, ensuring network security, and direct marketing where appropriate. We will always consider whether your rights outweigh our interests before processing on this basis.
 - (g) We process your personal information if it is necessary to protect your life or in a medical situation, it is necessary to carry out a public function, a task of public interest or if the function has a clear basis in law.
 - (h) We do not collect or process any personal information from you that is considered "Sensitive Personal Information" under the GDPR, such as personal information relating to your sexual orientation or ethnic origin unless we have obtained your explicit consent, or if it is being collected subject to and in accordance with the GDPR.
 - (i) You must not provide us with your personal information if you are under the age of 16 without the consent of your parent or someone who has parental authority for you. We do not knowingly collect or process the personal information of children.
- (g) Your rights under the GDPR
- (a) If you are an individual residing in the EU, you have certain rights as to how your personal information is obtained and used. Publishd PTY LTD complies with your rights under the GDPR as to how your personal information is used and controlled if you are an individual residing in the EU
 - (b) Except as otherwise provided in the GDPR, you have the following rights:
 - (i) to be informed how your personal information is being used;
 - (ii) access your personal information (we will provide you with a free copy of it);
 - (iii) to correct your personal information if it is inaccurate or incomplete;
 - (iv) to delete your personal information (also known as "the right to be forgotten");
 - (v) to restrict processing of your personal information;
 - (vi) to retain and reuse your personal information for your own purposes;
 - (vii) to object to your personal information being used; and
 - (viii) to object against automated decision making and profiling.
 - (c) Please contact us at any time to exercise your rights under the GDPR at the contact details in this Privacy Policy.
 - (d) We may ask you to verify your identity before acting on any of your requests.
- (h) Hosting and International Data Transfers
- (a) Information that we collect may from time to time be stored, processed in or transferred between parties or sites located in countries outside of Australia. These may include, but are not limited to Australia, United States, United Kingdom, and Germany. For each of these transfer destinations, we implement the following safeguards:

- (i) United States — transfers are protected via Standard Contractual Clauses (SCCs) approved by the European Commission and, where applicable, supplementary technical measures including end-to-end encryption;
 - (ii) United Kingdom — transfers are conducted in accordance with the UK GDPR and the UK International Data Transfer Agreement (IDTA) as approved by the UK Information Commissioner's Office; and
 - (iii) Germany — as a member of the European Economic Area (EEA), transfers to Germany are not restricted under the GDPR. All transfers are subject to ongoing risk assessments to ensure an equivalent level of data protection is maintained.
 - (b) We and our other group companies have offices and/or facilities in Australia, United States, United Kingdom, and Germany. Transfers to each of these countries will be protected by appropriate safeguards, these include one or more of the following: the use of standard data protection clauses adopted or approved by the European Commission which you can obtain from the European Commission Website; the use of binding corporate rules, a copy of which you can obtain from Publishd PTY LTD's Data Protection Officer.
 - (c) The hosting facilities for our website are situated in Australia, United States, United Kingdom, and Germany. Transfers to each of these Countries will be protected by appropriate safeguards, these include one or more of the following: the use of standard data protection clauses adopted or approved by the European Commission which you can obtain from the European Commission Website; the use of binding corporate rules, a copy of which you can obtain from Publishd PTY LTD's Data Protection Officer.
 - (d) Our Suppliers and Contractors are situated in Australia, United States, United Kingdom, and Germany. Transfers to each of these Countries will be protected by appropriate safeguards, these include one or more of the following: the use of standard data protection clauses adopted or approved by the European Commission which you can obtain from the European Commission Website; the use of binding corporate rules, a copy of which you can obtain from Publishd PTY LTD's Data Protection Officer.
 - (e) You acknowledge that personal data that you submit for publication through our website or services may be available, via the internet, around the world. We cannot prevent the use (or misuse) of such personal data by others.
 - (f) Where we transfer personal data to countries outside the European Economic Area (EEA), we implement additional technical and organisational measures including encryption of data in transit, regular security assessments of recipients, and contractual safeguards through Standard Contractual Clauses (SCCs) as approved by the European Commission under Article 46 of the GDPR.
- (i) Security of your personal information

- (a) Publishd PTY LTD is committed to ensuring that the information you provide to us is secure. In order to prevent unauthorised access or disclosure, we have put in place suitable physical, electronic and managerial procedures to safeguard and secure information and protect it from misuse, interference, loss and unauthorised access, modification and disclosure.
- (b) Where we employ data processors to process personal information on our behalf, we only do so on the basis that such data processors comply with the requirements under the GDPR and that have adequate technical measures in place to protect personal information against unauthorised use, loss and theft.
- (c) The transmission and exchange of information is carried out at your own risk. However, Publishd PTY LTD implements the following technical and organisational security measures to protect your personal information during transmission and storage:
 - (i) **Encryption in transit** - We protect data in transit using industry-standard encryption. Access to the Send Files website and web application uses HTTPS with TLS 1.2 or higher. File uploads to our servers are typically made over SFTP, which encrypts the connection using SSH. API communication between our application services and our providers (including Cloudflare, Backblaze, and AWS) also uses encrypted connections. When you configure sync to external destinations, encryption in transit depends on the protocol and settings you choose (for example, FTPS/TLS); we recommend using encrypted connection options where available.
 - (ii) **Encryption at rest** - Provider-managed encryption at rest on Backblaze B2, Cloudflare (D1/KV/R2), and AWS Rekognition; AES-256-GCM for selected stored credentials.
 - (iii) **Access controls** - we implement strict role-based access controls to ensure that personal information is only accessible to authorised personnel;
 - (iv) **Regular security assessments** - we conduct periodic security audits and vulnerability assessments of our systems and infrastructure; and
 - (v) **Incident response** - we maintain a data breach response plan in accordance with the Privacy Act 1988 (Cth) and the GDPR.
 - (vi) **Third-party processor agreements** - we maintain written Data Processing Agreements (DPAs) with all third-party processors (including AWS, Cloudflare, Backblaze, and payment providers) that comply with GDPR Article 28 requirements, specifying data protection obligations, security measures, audit rights, and liability allocation, and we will notify you of any material changes to our sub-processors.

Notwithstanding the above measures, we cannot guarantee the absolute security of any information transmitted to or from us. Although we take all reasonable steps to safeguard against unauthorised disclosures of information, we cannot assure you that personal information we collect will not be disclosed in a manner inconsistent with this Privacy Policy. If you suspect any misuse, loss, or unauthorised access to your personal information, please contact us immediately at support@send-files.com.

In the event of a data breach that is likely to result in a risk to the rights and freedoms of individuals, we will notify the relevant supervisory authority within 72 hours of becoming aware of the breach, in accordance with GDPR Article 33(1). Where the breach is likely to result in a high risk to affected individuals, including photographers whose portfolio data or clients whose project information is compromised, we will notify those individuals without undue delay and within 30 days of breach confirmation. All breaches will be documented in our breach register, including the nature of the breach, affected data categories, likely consequences, and remedial actions taken.

- (d) In the event of a personal data breach, we will notify the relevant supervisory authority within [HOURS] hours of becoming aware of the breach, where feasible. If the breach is likely to result in a high risk to your rights and freedoms, we will also notify affected individuals without undue delay, including a clear description of the breach's nature and recommendations to mitigate potential adverse effects.
- (e) **Limitation of Liability** — To the maximum extent permitted by law, and subject to any rights you may have under the Australian Consumer Law or applicable data protection legislation (including the Privacy Act 1988 (Cth) and the GDPR), Publishd PTY LTD's liability for any data breach or unauthorised access is limited to direct damages not exceeding the total fees paid by you in the 12 months preceding the incident. We are not liable for losses resulting from your failure to maintain secure credentials, follow recommended security practices, or comply with access control measures. Our total liability for any data-related claim is capped at 12 months of fees paid, excluding liability for indirect, consequential, or punitive damages. These limitations do not apply to:
 - (i) our gross negligence or wilful misconduct;
 - (ii) any liability that cannot be excluded or limited under the Australian Consumer Law;
 - (iii) any liability arising from our failure to comply with the notifiable data breach scheme under Part IIIC of the Privacy Act 1988 (Cth); or
 - (iv) any liability arising from our obligations as a Data Processor under the GDPR, including in respect of biometric data processing.

In the event of a data breach that is likely to result in a risk to the rights and freedoms of individuals, we will notify the relevant supervisory authority within 72 hours of becoming aware of the breach, in accordance with GDPR Article 33(1) and the notifiable data breach scheme under the Privacy Act 1988 (Cth). Where the breach is likely to result in a high risk to affected individuals, including photographers whose portfolio data or clients whose project information is compromised, we will notify those individuals without undue delay and within 30 days of breach confirmation. All breaches will be documented in our breach register, including the nature of the breach, affected data categories, likely consequences, and remedial actions taken.

(j) Access to your personal information

- (a) You may request details of personal information that we hold about you in accordance with the provisions of the *Privacy Act* 1988 (Cth), and to the extent applicable the EU GDPR. If you would like a copy of the information which we hold about you or believe that any information we hold on you is inaccurate, out of date, incomplete, irrelevant or misleading, please email us at support@send-files.com.
- (b) We reserve the right to refuse to provide you with information that we hold about you, in certain circumstances set out in the Privacy Act or any other applicable law.

(k) Complaints about privacy

- (a) If you have any complaints about our privacy practices, please feel free to send in details of your complaints to support@send-files.com. We take complaints very seriously and will respond shortly after receiving written notice of your complaint.

(l) Changes to Privacy Policy

- (a) Please be aware that we may change this Privacy Policy in the future. We may modify this Policy at any time, in our sole discretion and all modifications will be effective immediately upon our posting of the modifications on our website or notice board. Please check back from time to time to review our Privacy Policy.

(m) Website

(a) *When you visit our website*

When you come to our website (www.send-files.com), we may collect certain information such as browser type, operating system, website visited immediately before coming to our site, etc. This information is used in an aggregated manner to analyse how people use our site, such that we can improve our service.

- (b) **Cookies** - We may from time to time use cookies on our website. Cookies are very small files which a website uses to identify you when you come back to the site and to store details about your use of the site. Cookies are not malicious programs that access or damage your computer. Most web browsers automatically accept cookies but you can

choose to reject cookies by changing your browser settings. However, this may prevent you from taking full advantage of our website. Our website may from time to time use cookies to analyse website traffic and help us provide a better website visitor experience. In addition, cookies may be used to serve relevant ads to website visitors through third party services such as Google AdWords. These ads may appear on this website or other websites you visit.

(c) We categorise cookies used on our website as follows:

- (i) Strictly Necessary cookies required for basic site functionality;
- (ii) Performance cookies that help us analyse and improve our website;
- (iii) Functional cookies enabling enhanced personalised features; and
- (iv) Targeting/Advertising cookies used to deliver personalised content and advertisements.

You can manage your cookie preferences through our Cookie Control Panel, where you may enable or disable non-essential cookies. We will always request your explicit consent before placing non-essential cookies on your device, and you may withdraw this consent at any time through your browser settings or our Cookie Control Panel. For users in the EU, our cookie consent mechanism complies with the requirements of the GDPR and the ePrivacy Directive. A full list of cookies used on our website is available upon request by contacting us at support@send-files.com.

(d) *Third party sites*

Our site may from time to time have links to other websites not owned or controlled by us. These links are meant for your convenience only. Links to third party websites do not constitute sponsorship or endorsement or approval of these websites. Please be aware that Publishd PTY LTD is not responsible for the privacy practises of other such websites. We encourage our users to be aware, when they leave our website, to read the privacy statements of each and every website that collects personal identifiable information.

(n) Effective date

This policy is effective from 23 Jun 2026.