

Privacy Policy

Introduction

DataShift Pty Ltd ("**DataShift**", "**we**", "**us**" or "**our**") is an Australian company that develops software and integration solutions for businesses, including electronic data interchange (EDI) document automation and generalised software integration services. Our customers operate primarily in Australia but may also be located in other jurisdictions. When you engage with our products and services or visit our websites (collectively, **Services**), we collect, use and process information about your organisation and individuals acting on your behalf (**you** or **your**).

1. Open and transparent management of personal information

DataShift is committed to managing personal information in an open and transparent way. Australian Privacy Principle 1 requires organisations to have an up-to-date and publicly available privacy policy that explains what personal information is collected, how it is used and how individuals can access, correct or complain about the handling of their information. This policy fulfils that obligation.

2. What information we collect

We collect information necessary to provide the Services and run our business. Depending on the context, the information may include:

- **Contact and account information** – names, job titles, business addresses, telephone numbers, email addresses, user names and authentication credentials (including multi-factor authentication tokens).
- **Business and transaction data** – purchase orders, invoices, EDI documents, integration data, billing and payment records, tax identifiers, organisational details and usage metrics.
- **Payment information** – while payments are processed through third-party providers such as Stripe, we may collect limited billing details (e.g., billing contact, partial card numbers, tax information) to facilitate invoicing and reconciliation.

- **Technical information** – IP addresses, device and browser details, log files, usage data, and information collected through cookies and similar technologies.
- **Other information you provide** – communications with us, responses to surveys or support queries, and information supplied when signing agreements or participating in demos.

We only collect personal information that is reasonably necessary for our functions or activities. Sensitive information (e.g., information about health, race or criminal records) is only collected with consent or when required by law.

3. How we collect information

- **Directly from you** – when you register an account, interact with our staff, submit EDI documents, purchase our Services, enter data into our platform, respond to surveys or contact us for support.
- **From your organisation** – if you are an employee or authorised representative of a business customer, we may receive your details from that organisation.
- **Automatically** – we use cookies, logs and analytics to collect information about how you use our Services. Cookies help us understand usage patterns and improve our Services; where required by law, we will obtain consent.
- **From third parties** – we may receive information from payment processors, partners, public sources and data enrichment providers (e.g., company registries).

4. Why we collect and use information

We collect and use personal information for purposes including:

- **Service delivery and account management** – to create and manage user accounts, authenticate users (including enforcing two-factor authentication for authorised users), provide EDI integration and document automation services and develop new features.
- **Customer support and communications** – to respond to enquiries, provide technical support, send administrative messages and inform you about service updates. We may use email addresses or phone numbers to contact you.

- **Billing and payments** – to invoice customers, process payments via third-party providers, verify billing information, resolve payment issues and comply with taxation requirements.
- **Improving and developing our Services** – analysing usage data and feedback to understand trends and improve performance. We may use aggregated or de-identified data for analytics and research.
- **Marketing (with consent)** – to send you information about new products, services or promotions. Under APP 7, organisations may only use or disclose personal information for direct marketing with consent or if the individual would reasonably expect it. You can opt out of marketing communications at any time.
- **Security and fraud prevention** – to protect accounts and systems, detect and prevent unauthorised access, enforce our terms, and investigate misuse. We may log access information and use technical measures such as encryption and multi-factor authentication.
- **Legal compliance** – to comply with applicable laws, regulations and lawful requests (e.g., record-keeping obligations, law enforcement requests) and to manage disputes.

Under the GDPR, we rely on legal bases for processing personal data, including: (i) performing a contract with you or your organisation; (ii) our legitimate interests in providing and improving the Services, provided those interests are not overridden by individuals' rights; (iii) compliance with legal obligations; and (iv) where required, your consent. When consent is our legal basis, you may withdraw it at any time.

5. Use and disclosure of personal information

We only use or disclose personal information for the purpose for which it was collected or a related purpose that you would reasonably expect, with your consent, or as permitted or required by law. Examples of disclosures include:

- **Service providers** – we engage trusted third-party service providers to host our infrastructure, manage customer relationship systems, process payments, deliver communications, provide analytics, or support our operations. These providers may access personal information only to perform services on our behalf and are required to protect it.

- **Payment processors** – payments made through our platform are processed by third-party payment processors such as Stripe. We share necessary transaction details so payments can be completed.
- **Integration partners** – to facilitate EDI and integration services, we may transfer relevant data to trading partners, carriers, government agencies or other parties that you authorise.
- **Affiliates and advisors** – we may share information with our related entities, professional advisors (e.g., auditors, lawyers) and insurers for business purposes and to manage risk.
- **Legal requirements** – we may disclose information to courts, regulators, law enforcement or other third parties when we believe disclosure is required by law or to protect our rights and the rights of others.

We do not sell personal information. Where we use personal information for direct marketing, we comply with APP 7 requirements (including offering simple opt-out mechanisms). If you tell us you do not wish to receive marketing communications, we will respect your request.

6. Cross-border disclosure of personal information

DataShift is headquartered in Australia but operates globally. We may store or process personal information on servers located outside Australia or disclose information to overseas service providers. Under APP 8, before disclosing personal information overseas we must take reasonable steps to ensure the overseas recipient does not breach the APPs. The disclosing organisation generally remains liable for any acts of the overseas recipient that would breach the APPs, unless:

- we reasonably believe the recipient is subject to a law or binding scheme substantially similar to the APPs;
- you expressly consent to the transfer after being informed that we will not be responsible for any subsequent breaches; or
- another exception under the Privacy Act applies.

When transferring personal data outside the European Economic Area (EEA) under the GDPR, we implement appropriate safeguards such as standard contractual clauses approved by the European Commission, rely on adequacy decisions, or obtain your consent. We will provide information on the relevant transfer mechanism upon request.

7. Security of personal information

We take reasonable steps to protect personal information from misuse, interference, loss, and unauthorised access, modification or disclosure, as required by APP 11. Measures we use include:

- **Technical measures** – firewalls, intrusion detection, encryption of data in transit and at rest, secure development practices and vulnerability management. We require employees to use two-factor authentication on accounts that contain personal data.
- **Access controls** – role-based permissions, least-privilege access, and audit logs. We restrict access to personal information to staff who need it for their role.
- **Organisational measures** – staff training on data protection obligations, privacy policies and incident response. We maintain data protection and information security policies and review them periodically.
- **Physical security** – secure office premises and data centres with controlled access.

While we implement robust security measures, no method of transmission or storage is completely secure. If we become aware of a data breach that is likely to result in serious harm, we will notify the affected individuals and the Office of the Australian Information Commissioner (OAIC) as required by the Privacy Act's mandatory breach notification regime. Under the GDPR we will notify supervisory authorities and affected data subjects within 72 hours where required.

8. Anonymity and pseudonymity

APP 2 gives individuals the option of not identifying themselves or using a pseudonym when dealing with an organisation where it is lawful and practicable. You may choose to remain anonymous when making general enquiries. However, certain Services (such as account registration, payment processing and EDI integrations) require you to provide identifying information so we can authenticate you, provide access, and comply with legal obligations.

9. Access, correction and other rights

- **Access** – you can request access to personal information we hold about you. We will provide access unless an exception applies (e.g., providing access would unreasonably impact another person's privacy or is subject to legal privilege). We may charge a reasonable fee for providing access where permitted.
- **Correction** – you may ask us to correct inaccurate, out-of-date, incomplete or misleading information. We will take reasonable steps to correct the information and will notify relevant third parties if you ask us to and it is reasonable to do so.
- **Other rights under GDPR** – if the GDPR applies, you also have the right to request erasure of your data, restrict or object to processing, obtain a portable copy of your data, and not be subject to automated decision making or profiling. We will respond to such requests as required by law.
- **Opt-out of marketing** – you can opt out of receiving marketing communications at any time by following the unsubscribe instructions or contacting us. We will continue to send important transactional or administrative messages.

To exercise these rights, please contact us (see Section 15). We may need to verify your identity before processing a request.

10. Data retention and destruction

We retain personal information for as long as necessary to fulfil the purposes for which it was collected, including to provide the Services, comply with our legal obligations, resolve disputes, and enforce our agreements. When personal information is no longer needed for any lawful purpose, we take reasonable steps to destroy or permanently de-identify it.

11. Notifiable data breaches and cybersecurity incidents

If we suspect there has been an eligible data breach under Australia's Privacy Act or a personal data breach under GDPR, we will promptly assess the situation. An eligible data breach occurs when unauthorised access to or disclosure of personal information is likely to result in serious harm and remedial action cannot prevent the risk of harm. We will notify affected individuals and the OAIC of any eligible data breaches and provide a statement describing the breach, the information involved and steps

individuals should take. For GDPR-covered data subjects, we will notify the relevant supervisory authority within 72 hours of becoming aware of a notifiable breach, unless the breach is unlikely to result in a risk to individuals' rights and freedoms.

12. Children's privacy

The Services are intended for use by businesses and are not directed at children. We do not knowingly collect personal information from persons under 15 years of age. If we become aware that we have inadvertently collected information from a child without appropriate consent, we will delete it.

13. Third-party links and services

Our Services may contain links to or integrations with third-party websites and services that we do not operate. These may include payment gateways, EDI trading partners, analytics providers and content providers. When you interact with these third parties, their privacy practices apply. We encourage you to review their privacy policies. DataShift is not responsible for the privacy or security practices of third parties.

14. Changes to this Privacy Policy

We may update this policy from time to time to reflect changes in our practices, technology, legal requirements or other factors. When we make material changes, we will post the updated policy on our website and indicate the effective date. We may also notify you by email or through the Services. Your continued use of the Services after the effective date constitutes your acceptance of the updated policy.

15. Contacting us and complaints

If you have questions or concerns about this policy or our handling of personal information, or if you wish to exercise your rights, please contact our team.

Privacy & Compliance Team

DataShift Pty Ltd

support@datashift.com.au

We will respond to enquiries and complaints promptly. If you are dissatisfied with our response, you may lodge a complaint with the OAIC (for Australian residents) or the competent data protection authority in your jurisdiction.

Last Updated: 6 October 2025
