PRIVACY POLICY

This Privacy Policy applies to Precision Solutions Group Pty Ltd (ACN 629 448 773) and its subsidiaries (collectively referred to as "PSG," "we," "us," or "our"). This policy outlines how we collect, use, store, share, and protect personal information collected through our website, services, software platforms, and products, including those offered by our subsidiaries.

Last Updated: October 2024

COMPANY INFORMATION

PSG and its subsidiaries are committed to complying with all applicable Australian and international privacy laws, including the **Privacy Act 1988 (Cth), Australian Privacy Principles (APPs)**, the **General Data Protection Regulation (GDPR)**, and the **California Consumer Privacy Act (CCPA)**. This policy applies to all personal information that is collected, processed, and stored by PSG and its related entities.

Subsidiaries covered by this Privacy Principle include:

PSG IP Pty Ltd (ACN 629 456 186)

Cyber Intelligence Solutions Pty Ltd (ACN 629 452 419)

Securus Technology Pty Ltd (ACN 672 080 312)

Operational Intelligence Solutions Pty Ltd (ACN 629 454 191)

Development Capital Solutions Pty Ltd (ACN 673 392 455)

1. Collection of Personal Information

We collect personal information for legitimate business purposes, such as to provide you with our services and to comply with legal obligations. Personal information collected may include:

1.1. Personal Identifiable Information (PII): Full name, email address, phone number, physical address, and job title.

1.2. Financial Information: Payment details for transactions.

1.3. Technical Information: Internet Protocol (IP) address, browser type and version, operating system, device identifiers, cookie data, and website usage data.

1.4. Sensitive Information: In some cases, we may collect sensitive information such as identity verification details, which are protected under stricter guidelines.

1.5. We may also collect information indirectly from third parties, such as your employer, commercial partners, or service providers, to enhance or support the services you request.

2. Methods of Collection

2.1. Direct Collection: When you provide information via our contact forms, email, phone, or register for services or events.

2.2. Automatic Collection: Data is automatically collected when you visit our website, use our services, or access online resources. We use cookies, web beacons, and other tracking technologies (see Section 10).

2.3. Third-Party Sources: We may also collect data from third-party service providers, business partners, and publicly available sources to improve services and user experience.

3. Purpose of Collecting Personal Information

We collect and process personal information for the following purposes:

3.1. Service Provision: To deliver the services you request, including technical support and account management.

3.2. Transaction Processing: To manage your orders, process payments, and fulfil contracts.

3.3. Security & Risk Management: To safeguard our systems and your data from unauthorised access, fraud, and cyberattacks.

3.4. Compliance: To comply with legal and regulatory requirements, including GDPR and CCPA compliance.

3.5. Marketing & Communications: To send you marketing communications, newsletters, and promotional materials (only with your explicit consent).

3.6. Data Analytics & Service Improvement: To monitor website performance and improve our services, as well as to provide targeted advertising and content customisation (see Section 10 on Cookies).

4. Legal Basis for Processing

We process personal information under the following legal grounds:

4.1. Consent: This applies when a data subject has given clear and specific consent for the processing of their Personal Information for one or more specific purposes. Consent must be freely given, informed, and unambiguous. Users must have the ability to withdraw their consent at any time.

4.2. Contractual Necessity: This applies when we process Personal Information that is necessary for the performance of a contract to which the data subject is a party or for taking steps at the data subject's request prior to entering into a contract. This basis typically applies when Personal Information is processed to fulfill an agreement with the data subject such as commercial agreement.

4.3. Legal Obligation: This applies when we process Personal Information that is necessary for our compliance with a legal obligation. This basis is relevant when processing is required to fulfill a legal requirement imposed on us such as answering questions from a regulator.

4.4. Legitimate Interests: This basis applies when we process Personal Information that is necessary for the legitimate interests pursued by the controller or a third party, except where such interests are overridden by the data subject's interests or fundamental rights and freedoms. Examples of this basis include processing Personal Information to improve our service offerings, providing technical support, managing User feedback, and replying to User requests and complaints. When relying on legitimate interests, we use our best efforts to verify that the interests or rights of the data subject do not outweigh our legitimate interests

4.5. Service Provisions: In instances where we provide services that involve accessing or processing data from business systems (such as lists of users, including employees and guests, from platforms like Microsoft), the customer is responsible for ensuring that all individuals whose data is being processed have been adequately informed and, where applicable, have provided consent for their data to be used. This includes, but is not limited to, notifying staff and guests that their information may be monitored, stored, and processed as part of the customer's use of our services. We rely on the customer to comply with all applicable data protection laws, including informing data subjects about how their data will be processed. PSG will not be held liable for any failure by the customer to provide the necessary notice or obtain the required consent.

5. Disclosure of Personal Information

We do not sell your personal information. However, we may disclose your data to third parties under specific circumstances:

5.1. Service Providers: We engage with third-party service providers under contract who process data on our behalf. These providers include cloud hosting platforms, IT service providers, payment processors, and marketing agencies.

5.2. Business Partners: In cases where collaboration with third-party business partners is necessary for service delivery.

5.3. Legal Compliance: PSG may disclose personal information to law enforcement, regulatory agencies, or in response to legal processes such as subpoenas, to comply with applicable laws or protect our legal rights.

5.4. Legitimate Interests: In some cases, data sharing is necessary to fulfil our legitimate interests, provided this does not infringe on your rights. This could include improving service functionality, troubleshooting issues, or enhancing user experience.

5.5. Corporate Transactions: In the event of a merger, acquisition, sale, or transfer of assets, PSG may transfer personal data as part of the business transaction. In such a scenario, we will notify you and ensure that any entity receiving your data upholds privacy protections equivalent to those outlined in this policy.

5.6. Subsidiaries: We may share information between subsidiaries within the PSG group for seamless service provision.

All third-party disclosures are subject to contractual agreements to ensure the security and confidentiality of your data.

6. International Data Transfers

For international data transfers to countries outside Australia and the European Economic Area (EEA), PSG implements the following measures:

6.1. We assess the legal frameworks of destination countries to ensure they provide an adequate level of protection.

6.2. We incorporate additional contractual safeguards to ensure the safety of your data, even when it is transferred to jurisdictions that do not have stringent data protection laws.

6.3. In cases where third-party service providers are located in countries without adequate data protection laws, we require that they implement the same security and privacy controls to safeguard personal data.

PSG ensures that appropriate safeguards are in place for cross-border data transfers, including:

6.4. Standard Contractual Clauses (SCCs): For transfers outside the European Economic Area (EEA), we utilise SCCs approved by the European Commission.

6.5. Binding Corporate Rules (BCRs): For intra-group data transfers within PSG entities.

Where necessary, we will seek explicit consent for international transfers, especially in regions governed by the GDPR.

7. Data Retention

We retain personal information only for as long as necessary to fulfil the purposes outlined in this policy, or to comply with legal, regulatory, or contractual obligations. The retention periods are:

7.1. Transactional Data: Retained for seven (7) years in accordance with tax and accounting regulations.

7.2. Marketing Data: Retained until you opt out of communications or withdraw your consent.

7.3. Security Logs: Retained for up to twelve (12) months for forensic and compliance purposes.

7.4. Other Data: Retained as long as required for legal or regulatory compliance.

Once the retention period expires, data is securely deleted or anonymised.

8. Security

PSG takes the protection of your personal information seriously and implements industry-standard encryption protocols. We align with the International Standard for Information Security, ISO27001, as well as that relating to Privacy, ISO27701. This involves setting up a system to manage risk around both information security and data protection / privacy, as well as putting in place measures and objectives to keep improving. This includes:

8.1. Encryption in Transit: All personal data transmitted across our platforms is encrypted using TLS 1.2 or higher, ensuring secure data transfer between your device and our systems.

8.2. Encryption at Rest: All sensitive personal data is encrypted at rest using AES-256 encryption. Access to this data is strictly limited to authorized personnel.

8.3. Access Control: We implement conditional role-based access control (RBAC), ensuring that only authorised personnel have access to sensitive data, and access logs are regularly audited.

8.4. Multi-Factor Authentication (MFA): We use MFA to provide an extra layer of security for account access.

8.5. Regular Security Audits: Our systems undergo regular security assessments, including penetration tests and audits, to identify and mitigate vulnerabilities.

8.6. Incident Response: In the event of a data breach involving personal information, PSG is committed to complying with the Notifiable Data Breaches (NDB) scheme under the Privacy Act 1988 (Cth). If the breach is likely to result in serious harm, PSG will notify affected individuals, and the Office of the Australian Information Commissioner (OAIC) as required by law.

While we strive to ensure the security of personal information, it is important to note that no system or transmission method can guarantee complete security. Despite our best efforts, unauthorised access or breaches may still occur.

9. Your Rights

Under applicable privacy laws, you have several rights regarding your personal information:

9.1. Access: You have the right to request a copy of the personal data we hold about you.

9.2. Correction: You can request corrections or updates to your personal information if it is inaccurate or outdated.

9.3. Deletion: You have the right to request that we delete your personal information, provided we are not required to retain it by law.

9.4. Data Portability: You may request that your personal data be provided to you in a structured, machine-readable format for transfer to another service provider.

9.5. Objection: You have the right to object to the processing of your data for direct marketing purposes or if the processing is based on legitimate interests.

9.6. Restrict Processing: You may request that we restrict the processing of your data under certain circumstances, such as when contesting its accuracy.

9.7. Withdraw Consent: If we process your data based on consent, you have the right to withdraw that consent at any time.

To exercise these rights, please contact privacy@psg.ltd. We will respond to your request within the applicable statutory time limits.

10. Cookies and Tracking Technologies

We use cookies and similar technologies to enhance your experience on our website. These may include:

10.1. Strictly Necessary Cookies: Essential for website functionality.

10.2. Performance Cookies: Used to measure website performance and understand user behaviour.

10.3. Targeting Cookies: Used for advertising purposes and to track user interactions across different websites.

You can control cookie settings through your browser. However, disabling cookies may affect the functionality of our website.

11. Automated Decision Making and Profiling

PSG does not engage in automated decision-making processes that have legal or similarly significant effects on individuals. However, we may use profiling techniques for marketing purposes to tailor our services and communications to your preferences, but only with your consent.

12. Minors

Our services are not intended for individuals under the age of 18. We do not knowingly collect personal information from minors. If you believe that a minor has provided us with personal information, please contact us at privacy@psg.ltd, and we will take steps to delete the information.

13. Third Party Websites

Our website may contain links to third-party websites. PSG is not responsible for the privacy practices of third-party websites. We encourage you to review the privacy policies of each website you visit.

14. Changes to the Privacy Policy

We may update this Privacy Policy from time to time to reflect changes in our practices or legal requirements. Any changes will be posted on this page with the updated "Effective Date." If the changes are significant, we will notify you via email or a prominent notice on our website.

15. Contact Information

If you have any questions about this Privacy Policy or wish to exercise your privacy rights, please contact our Data Protection Officer:

Privacy Officer
PSG Group
Level 17 Chifley Tower, 2 Chifley Square, Sydney NSW 2000
Email: **privacy@psg.ltd**
Phone: +61 2 9375 2140