

SSP Australia Privacy Policy (Australia)

Effective date: 1 April 2026

Entities: SSP Australia Catering Pty Ltd (ABN 75 134 475 924)

Airport Retail Enterprises Pty Ltd (ABN 16 008 749 031)

Privacy contact: dataprotection@ssp-au.com

CCTV Request contact: cctv.request@ssp-au.com

Postal address: Suite 405/83 York Street, Sydney NSW 2000

This Privacy Policy applies to personal information collected, held, used, accessed, stored, processed and/or disclosed by SSP Australia in connection with our operations in Australia, including our food and beverage venues in travel and airport locations across Australia.

This Privacy Policy explains our practices in accordance with:

- The Australian Privacy Act 1988 and Australian Privacy Principles (APPs)
- The UK General Data Protection Regulation (UK GDPR) and UK Data Protection Act 2018 (where applicable)
- The EU General Data Protection Regulation (EU GDPR)(Regulation (EU) 2016/679) (where applicable).

SSP Australia operates as part of the SSP Group plc, a multinational company headquartered in the United Kingdom, with regional operations managed through SSP Asia Pacific Limited. Because we operate within an international group structure and use service providers located outside Australia, compliance with all of the abovementioned data protection laws is essential for our lawful processing of your personal data, lawful cross-border data transfers (e.g. to the UK, Hong Kong, EU/EEA, the US and India) and group-wide governance.

1. Purpose and who we are

We are committed to handling personal information in an open, transparent and lawful manner. This Privacy Policy explains how SSP Australia Catering Pty Ltd (ABN 75 134 475 924) and Airport Retail Enterprises Pty Ltd (ABN 16 008 749 031) (together "SSP Australia", "we", "us", "our") collects, holds, uses, stores, processes and discloses personal information in connection with our Australian operations (including our food and beverage venues and activities in the travel and airport hospitality environment).

1.1 Who we are

SSP Australia operates food and beverage outlets in travel locations in Australia. We are part of a multinational corporate group, forming part of the Select Service Partner Asia Pacific Limited region (an APAC head office located in Hong Kong) and global SSP Group plc (our parent company headquartered in the United Kingdom) (altogether, the "SSP Group"). Because we operate as part of an integrated international group and use service providers (including SaaS cloud software), personal information may be processed, accessed or stored outside Australia including in the UK, the EU, Hong Kong, and other countries where SSP Group operates or where service providers are located.

See section 7. for detailed information about international data transfers and safeguards.

1.2 Controller and Data Protection Responsibility

For the purpose of this Privacy Policy, SSP Australia is the APP entity responsible for personal information collected through our Australian operations under Australian Privacy Act and is the data controller as defined under EU GDPR and UK GDPR.

In certain circumstances, SSP Australia may act as a joint controller with other SSP Group entities (e.g. where we jointly determine purposes and means of processing for group-wide systems, shared customer databases or consolidated reporting). Where joint controller arrangements exist, SSP Australia and the relevant SSP Group entities clearly allocate and document their respective responsibilities in accordance with applicable data protection laws.

2. Key definitions

This Privacy Policy uses terminology drawn from Australian, EU and UK data protection laws in accordance with the definitions listed in Appendix A attached herein.

3. Personal information we collect and store

3.1 Categories of Personal Data and to Who They Apply To

The categories and types of personal information we collect depend on how you interact with us and your relationship with SSP Australia. Below is a summary table of the information that we collect:

Categories of Personal Data	Categories of Data Subject	Types of Personal Data Collected
Identity Data	Customers and visitors, suppliers, contractors and business contacts	includes your first name, maiden name, last name, any middle names, username or similar identifier, marital status, title, date of birth and gender
Contact Data	Customers and visitors, suppliers, contractors and	includes your billing address, delivery address, email address and telephone numbers

	business contacts, job applicants	
Financial Data	Customers and visitors, suppliers, contractors and business contacts	includes your credit card number, debit card number, bank account and any other payment card details
Transaction Data	Customers and visitors, suppliers, contractors and business contacts	means the date, time, location and amount of each transaction, the details of products and services you purchase from us, your membership ID (if applicable) and any information required to process benefits or redemptions (for example loyalty or lounge-access programs).
Technical & Usage Data	Customers and visitors, Suppliers, contractors and business contacts, job applicants	means information such as your internet protocol (IP) address, login data, browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform and other technology on the devices you use to access our website or our Wifi services. It also includes information about how you use our website, network usage or diagnostic logs required to operate and secure the device and connection timestamps or session duration.
Profile Data	Job applicants, Customers and visitors	means your username and password created on our Career site, your interests, preferences, and feedback and survey responses
Complaints & Opinions	Customers and visitors, Suppliers, contractors and business contacts, job applicants	means enquiries, complaints, feedback or opinions you submit to us, together with the contact information you provide.
Safety and Security Incident Data	Customers and visitors, Suppliers, contractors and business contacts	Means records relating to safety or security incident records, which may include names, contact details, witness statements, and (where relevant) injury or health information

CCTV Data	Customers and visitors, Suppliers, contractors and business contacts	means images and/or video recordings that may show your physical appearance (including facial images, clothing, physical characteristics), together with associated metadata such as the date, time, location, camera identifier and recording duration.
Job Application Data	Job applicants	Means information you provide to us during a recruitment or hiring process, including your employment history and work experience, education information and qualifications, your curriculum vitae (CV) or resume, cover letters, referee contact details and feedback, interview notes and assessment records, results of screening checks (such as right to work verification, or criminal history checks), professional licenses or certifications and documents relating to your eligibility to work (such as visa status, work permits)

3.2 Special Category Data/ Health Data

In limited circumstances, we collect special category data (as defined under EU GDPR and UK GDPR), which is also known as sensitive information (as defined under the Australian Privacy Act). Such limited circumstances include:

- In the case where safety incidents occur involving injury, illness or medical emergency, provision of first aid, incident reports documenting health impacts and injuries, and/or
- when job applicants disclose medical conditions requiring workplace accommodation.
- where CCTV surveillance systems capture facial images of all individuals in surveilled venue areas, as well as CCTV footage and photographs which may inadvertently reveal racial or ethnic origin through visual appearance.
- during the recruitment process, where we may require police checks, criminal history checks, or working with children checks as mandated by Australian law.

Examples of which include:

- descriptions of injuries sustained in accidents at our venues
- medical conditions relevant to incident response (e.g. allergies, pre-existing conditions affecting first-aid)
- First-aid treatment records

- Health information voluntarily disclosed by job applicants (e.g. disability requiring reasonable accommodation)
- Pandemic-related health information (if collection is legally required)
- Visa or immigration status checks
- National police check results (where role requires)

3.3 Children's Personal Information

Our services are not directed at children under the age of 18 (or any lower age permitted by applicable data-protection laws). We do not knowingly collect personal information from children through our website or online services. CCTV systems at our venues may inadvertently capture images of children; such data is processed solely for safety and security purposes.

If you believe we have collected personal information from a child without appropriate consent, please contact us at dataprotection@ssp-au.com and we will take steps to delete it.

3.4 Consequences of Not Providing Personal Information

You are not obligated to provide personal information in most circumstances. However, failure to provide certain personal information may result in:

- Inability to provide products and services to you
- Inability to respond to your inquiry, complaint, or feedback
- Inability to process your job application or assess your suitability for employment
- Inability to provide Wi-Fi services (if you do not accept terms requiring Technical Data collection)
- Inability to investigate or respond to safety/ security incidents involving you
- Inability to fulfill legal or regulatory obligations
- Inability to establish or manage supplier/ contractor relationships

We do not currently operate online ordering, customer loyalty programs, or customer mailing lists in Australia.

4. How we collect personal information

We use different ways to collect personal information including through:

- Directly from you (in person, by phone or email, in forms you complete, or during complaint or incident handling, interacting with us, using our facilities and/or services at our venues).
- Through CCTV and site security/safety systems.
- Through Wi-Fi systems where provided at a site.
- Access to our website

- From third parties or publicly available sources where necessary and lawful (for example, insurers; your employer if you are a contractor representative; referees for recruitment, analytics and search engine providers such as Google, identity and contact data from publicly available sources).

In addition to this Privacy Policy, we provide collection notices (sometimes called privacy collection statements) at or before the time we collect personal information (or as soon as practicable afterwards), for example on forms, online portals (including recruitment), Wi-Fi landing pages, and via signage for CCTV.

4.1 Unsolicited personal information

Should we receive personal information we did not solicit, we will assess whether we could have collected it. If not, we will destroy or de-identify it where lawful and reasonable to do so.

5. Why we collect, hold, use and disclose personal information

We collect, hold, use, process, store and disclose personal information only for specified, explicit and legitimate purposes in accordance with the purpose limitation principle and with reference to the legal basis available under data protection law. Such legal basis include:

- **Consent:** when you give us your consent, we will process your personal data for the specific purpose you have consented to.
- **Performance of Contract:** when making products and/ or services available to you, we will process your personal data necessary for fulfilment of a contract (such as sales of food at our POS) with you and to fulfil any obligations derived from that contract; where we need to perform a contract; or where we are about to enter into or have entered into with you.
- **Legitimate interest:** Where we rely on legitimate interests, those interests may include: operating our venues safely and efficiently; preventing fraud, theft and loss; ensuring network and information security; protecting staff and customers; investigating incidents and complaints; and improving our services. Our legitimate interests do not outweigh your interests and fundamental rights as granted by the data protection laws.
- **Legal obligation:** whenever it is necessary for us to comply with a legal or regulatory obligation of the country of operation.
- **Vital interests:** in exceptional circumstances, we may process personal information where necessary to protect the vital interests of you or another person for example, in a medical emergency at one of our venues).

We may process your personal information on more than one lawful ground depending on the specific purpose for which we are using your personal information:

Purpose/ Activity	Type of Data	Legal Basis for Processing
When you register an account on our Career Site and/or when you apply for a job with us	(a) Identity Data (b) Contact Data (c) Profile Data (d) Job Application Data	(a) Consent (b) Legitimate Interest
Purchase/ Service-related Purposes such as processing payments, fees and charges.	(a) Identity Data (b) Contact Data (c) Financial Data (d) Transaction Data (e) Marketing and Communications Data	(a) Performance of Contract (b) Legitimate Interests
To manage our relationship and communication with you	(a) Identity Data (b) Contact Data	(a) Consent (b) Legitimate Interests
Service/ Product Improvement-related purposes such as collection of your opinion via surveys	(a) Identity Data (b) Contact Data (c) Marketing and Communications Data (d) Technical Data	(a) Consent (b) Legitimate Interests
Regulatory and legal obligations related purposes	(a) Identity Data (b) Contact Data (c) CCTV Data (d) Employment Data (e) Technical Data (f) Financial Data (g) Transaction Data	(a) Legal Obligation (b) Legitimate Interests
CCTV surveillance related purposes such as loss prevention, crime detection and prevention, for the personal safety of guests, employees and other members of the public, etc.	CCTV Data	Legitimate interests
Wi-Fi at our units	Technical Data	(a) Legitimate interests (b) Consent (where applicable)
Health & Safety Incident	(a) Identity Data	(a) Consent

Investigation	(b) Contact Data (c) CCTV Data (d) Employment Data (e) Technical Data (f) Financial Data (g) Transaction Data	(b) Legal Obligation (c) Legitimate Interests
---------------	--	--

6. Who we disclose personal information to

We may disclose your personal information with the third parties set out below for the purposes set out in section 5 above:

- **Within SSP:** to the extent permitted by law and the consent that you have given (if any), your personal information will only be accessible by a limited number of recipients within SSP. Such information access will strictly take place on a “need-to-know” basis in order for the recipients to fulfill the processing purposes in their capacity as data controllers.
- **Airport/landlord operators and their security or operations teams** where necessary for safety, security, access management or incident response.
- **Service providers** who support our usual business operations (including IT, Wi-Fi providers, CCTV/security contractors, HR system, incident management system providers, investigators, auditors, insurers, and professional advisers).
- **Regulators, government agencies, law enforcement, and courts/tribunals:** where required or authorised by law.
- There may be **other third parties** which may process your personal information for their own purposes (e.g. social media platforms such as Facebook, LinkedIn and Instagram). The processing by these entities is governed by their own privacy policies. You may check with privacy policies to understand how they manage your personal information. For avoidance of doubt, we do not disclose your personal information to these platforms unless you have consented or if we have a legitimate interest to do so.

We do not sell personal information. We do not store full payment card numbers or CVV details; payments are processed by our payment service providers.

7. International Transfers

We may share, disclose and/or transfer your personal information to overseas recipients. The level of data protection provided by these countries may vary. Below is the list of third parties to whom we may disclose your personal data:

- **related entities within SSP outside Australia:** your personal information will only be accessible by a limited and defined number of recipients within the SSP for the purpose of corporate governance, reporting, operations, administrative support, etc.; and/or
- **our service providers:** for providing products and/or services in support of our normal business operations e.g. to carry out IT-related tasks, conducting our business, servicing you, protecting and securing our business, etc.
- **Government agencies, law enforcement, courts and other public authorities etc.:** in limited cases, where we are legally required or permitted to do so, to respond to claims, or to protect our rights, interests, privacy, property or safety pursuant to applicable laws and regulations.
- **Other digital platforms:** there may be other third parties which may process your Personal Data for their own purposes (e.g. social media platforms such as Facebook, TikTok and Instagram), to the extent permitted by this policy. The processing by these entities is governed by their own privacy policies. You may check their privacy policies to understand how they manage your personal data. For avoidance of doubt, we do not disclose your personal data to these platforms unless you have consented so or if we have a legitimate interest to do so.

Before disclosing personal information to an overseas recipient, we take reasonable steps to ensure the recipient handles the information consistently with the Australian Privacy Principles unless an exception applies under the Privacy Act, and we acknowledge the accountability framework that may apply to overseas disclosures.

In any event, such data transfers will only occur where there is an applicable adequacy decision, the adoption of Standard Contractual Clauses (SCCs) and/or ASEAN Model Contractual Clauses (ASEAN MCCs), Binding Corporate Rule (BCRs), Certification and appropriate contractual clauses such as data processing agreement/ data transfer agreement.

Currently, we only transfer your personal information outside Australia for the destinations and purposes listed below using the transfer mechanisms described below:

Destination	Purpose	Transfer Safeguards
United Kingdom	SSP Group governance and administrative support, IT-related services and support within SSP Group and by third party service provider	Intragroup Data Transfer Agreement; adequacy decision, Data Processing Agreements incorporating SCCs.
Hong Kong	SSP APAC governance and administrative support, operational support	Intragroup Data Transfer Agreement
European Union/ EEA	SSP Group governance and reporting; IT-related services provided by third party service providers	Intragroup Data Transfer Agreement; Data Processing Agreement incorporating SCCs
United States	IT-related services/ SaaS provided by third party service providers	Data Processing Agreement incorporating SCCs
India	IT-related services/ SaaS provided by third party service providers	Data Processing Agreement incorporating SCCs

8. Direct marketing

SSP Australia does not currently operate customer direct marketing mailing lists or send promotional communications to customers in Australia. If this changes in the future, we will update this Privacy Policy to explain what personal information we collect for marketing purposes, how it is used, and how you can opt out. Any direct marketing will only be conducted with your consent or where otherwise permitted by the Spam Act 2003 (Cth) and the Do Not Call Register Act 2006 (Cth).

To the extent the SSP APAC Privacy Notice refers to marketing activities, those provisions do not currently apply to Australian operations unless and until we commence such activities and update this Privacy Policy accordingly.

9. Cookies and Tracking Technologies

Our website uses cookies and similar technologies (such as web server logs and web beacons) to collect Technical Data about how our website is used and your interactions with it.

What are cookies? Cookies are small text files placed on your device when you visit a website. They help us understand how visitors use our site, remember your preferences, and improve your experience.

Types of cookies we use:

Cookie Type	Purpose
Strictly necessary cookies	Essential for the website to function (e.g., session management, security). These cannot be switched off.
Preference cookies	These cookies remember your preferences and choices (such as language, region, or accessibility settings) to provide enhanced, personalised features.
Statistics cookies	Help us understand how visitors interact with our website by collecting information anonymously (e.g., pages visited, time on site). This helps us improve website performance and user experience.
Marketing/ advertising cookies	These cookies track your browsing activity across different websites to deliver personalised advertisements and measure advertising effectiveness.

Your choices: You can manage your cookie preferences through the cookie consent banner displayed on our website. You can also configure your browser settings to refuse or delete cookies. Please note that restricting cookies may impact your user experience and prevent you from using certain features of our website.

Third-party cookies: Our website may use analytics services such as Google Analytics, which set their own cookies. These services operate under their own privacy policies.

10. Camera Surveillance (CCTV)

10.1 General Provisions regarding CCTV

In our venues, we may use CCTV surveillance as a vital security measure to protect customers, employees, visitors and business. As such, we process images and videos that may capture your personal information through our CCTV systems. This personal information may be used to protect individuals, facilities, equipment, and all information contained within them from incidents, accidents, and malicious or criminal acts, and for loss prevention purposes.

Our CCTV operations comply with the Australian Privacy Act 1988 (Cth) and the relevant state and territory surveillance-device legislation, including (where applicable):

- Surveillance Devices Act 2007 (NSW) and Workplace Surveillance Act 2005 (NSW)
- Surveillance Devices Act 1999 (Vic)
- Invasion of Privacy Act 1971 (Qld)
- Surveillance Devices Act 2016 (SA)
- Surveillance Devices Act 1998 (WA)
- Listening Devices Act 1991 (Tas)
- Listening Devices Act 1992 (ACT)
- Surveillance Devices Act 2007 (NT)

We display clear signage at all venues where CCTV surveillance is in operation. Where required by applicable state or territory law (including the Workplace Surveillance Act 2005 (NSW)), we provide written notice to employees and ensure cameras are clearly visible. Audio recording via CCTV is only conducted where permitted under the applicable state or territory legislation.

10.2 Who may we disclose your CCTV Data?

Whilst all CCTV data is stored and processed locally in your country, we may share your personal information within the SSP Group and/or third parties (such as law enforcement agencies) where required to meet our legitimate interests or to comply with our legal obligations. This includes disclosure on request from police or where required under a court order or subpoena.

Access may also be provided to third-party security companies that supply installation and maintenance support services, as well as companies that provide loss prevention analysis services to SSP.

Any employees using CCTV will receive training to ensure that they understand and comply with the legal requirements relating to the processing of any CCTV information collected.

10.3 How long do we keep your CCTV Data?

Depending on the CCTV systems in use at our units, images and videos are retained for a period of approximately 20 to 30 days from the date of capture, unless longer retention period is required for internal investigation purposes or for evidencing acts that impact the safety of individuals, assets or facilities. In such cases, the relevant footage will be extracted from the system and retained for the duration of the investigation and/or any related proceedings.

We will ensure that CCTV Data collected is stored in a manner that maintains its integrity and security, which may include encrypting the CCTV Data where it is possible to do so.

10.4 Access to CCTV Footage

If you wish to exercise your right to access CCTV footage, please contact us at cctv.request@ssp-au.com or dataprotection@ssp-au.com. We may need to verify your identity before processing your request. We will respond within 30 calendar days (or within any shorter period required by applicable law). If we cannot fully comply with your request, we will explain the reasons and inform you of your right to make a complaint.

11. Anonymity and pseudonymity

Where lawful and practicable, you may interact with us anonymously or under a pseudonym. However, this may not be possible in circumstances involving safety or security incidents, CCTV requests or investigations, Wi-Fi access (depending on system configuration), recruitment processes, or where we are required or authorised by law to identify you.

12. Security and retention

We take reasonable steps to protect personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure. These steps include access controls, physical security, staff training, and supplier management.

We retain personal information only for as long as needed for the purposes described in this Privacy Policy, or as required by law. When personal information is no longer required, we take reasonable steps to destroy or de-identify it where lawful and reasonable. Where a mandated storage period under applicable laws (or a requirement of a regulatory or other competent body) expires, or where the purposes for which the information was collected no longer applies, the personal information will be deleted, de-identified or otherwise handled in accordance with legal requirements and our internal policies.

13. Your Privacy Rights

Depending on the laws that apply to you, you may have certain rights in relation to your personal information. To exercise any of these rights, contact us at dataprotection@ssp-au.com.

Privacy Rights	What does this mean?
Right to Confirm	You have the right to request confirmation of whether we hold personal information about you and whether we are processing that information.
Right to be Informed	You have the right to be informed in a clear and accessible way, about the personal information we collect, how we use it and the and for the purposes for which it is processed.
Right to Access	You have the right to access the personal information we hold about you. This includes information about the purposes of processing, the categories of personal information involved, and (where applicable) the types of recipients to whom it has been disclosed to the extent permitted by applicable law.
Right to Rectification	You have the right to request rectification of any personal information we hold about you that is inaccurate, out of date, incomplete or misleading. Where appropriate and taking into account the purposes for which the information is processed, you may also provide additional information to help us complete or update your personal information.
Right to Withdraw Consent	If you have provided consent for us to process your personal information, you may withdraw your consent at any time for future processing. Withdrawing your consent will not affect the lawfulness of any processing that occurred prior to the consent being withdrawn.
Right to Erasure (Right to be Forgotten)	In some cases, you have the right to erase your personal information without undue delay where one of the following grounds applies. However, this is not an absolute right and SSP Australia may have legal or legitimate grounds for retaining such personal information: • the personal information is no longer necessary in relation to the purposes for which it was collected or otherwise processed; • you withdraw your consent and there is no other legal basis for the processing; • you object to the processing and there are no overriding legitimate grounds for continuing the processing; • the personal information has been unlawfully processed.
Right to Restrict Processing	Where this right is provided under applicable data protection laws, you have the right to request the restriction of the processing of your personal information, where one of the following applies: • the accuracy of the personal information is contested by you, for a period enabling us to verify the accuracy of the

	personal information; • the processing is unlawful, and instead of requesting erasure you request the use of the personal information be restricted; • we no longer require the personal information for the purposes of processing but it is required under applicable laws, for the establishment, exercise or defence of legal claims. • you have objected to the processing pending verification of whether our legitimate grounds override your objections.
Right to Data Portability	Where this right is provided under applicable data protection laws, you have the right to receive personal information you have provided to us in a structured commonly used machine-readable format. You also have the right to transmit that personal information to another controller without undue hindrance from us. This right only applies where processing of your personal information is based on your consent or on a contract and where the processing is carried out by automated means.
Right to Object Processing	You have the right to object to the processing of your personal information where the processing is based on the legitimate interests of SSP Australia. SSP Australia may, however, rely on compelling legitimate grounds to continue processing. If you object to the processing of personal information for direct marketing purposes (if any), we will no longer process the personal information for those purposes.
Right to Object to Automated Decision-Making	As a general practice, SSP Australia does not use automated decision-making or profiling. However, where this right is granted under applicable data protection law, you have the right not to be subject to a decision based solely on automated processing without human involvement, where the decision produces legal effects concerning you, or significantly affects you. If such a decision is (a) necessary for entering into, or the performance of, a contract between you and us, or (b) based on your explicit consent, we will implement suitable measures to safeguard your rights, freedoms and legitimate interests. These measures may include the right to obtain human intervention on our part, to express your point of view and contest the decision.

Right to File Complaint	You have the right to lodge a complaint with the privacy regulator.
Right to deal with us anonymously or by pseudonym	Where lawful and practicable, you may choose not to identify yourself, or to use a pseudonym, when dealing with us (for example, when making general enquiries or providing feedback). However, in some situations we may need your real identity (for example, to process a payment, assess a job application, investigate an incident, or where we are required or authorised by law to verify your identity).

How to exercise your rights: You may submit your request by contacting dataprotection@ssp-au.com . We may need to verify your identity before processing your request. We will respond within 30 calendar days (or within any shorter period as required by applicable law). If we cannot fully comply with your request, we will explain the reasons and inform you of your right to complain.

Access and Correction (Australia): If you are an Australian resident, you may request access to, or correction of, the personal information we hold about you under the Privacy Act 1988 (Cth) by contacting us using the details in Section 13. We may need to verify your identity before processing your request. We will respond within a reasonable period and, where we refuse access or correction, we will provide written reasons (unless it would be unreasonable to do so) and explain how you can make a complaint to us and to the OAIC.

14. Automated Decision-Making

SSP Australia does not currently use solely automated decision-making (including profiling) that produces legal effects concerning you or similarly significantly affects you in our interactions with customers, suppliers, or job applicants.

If we introduce automated decision-making in the future, we will update this Privacy Policy to disclose:

- the kinds of personal information used in such automated systems;
- the kinds of decision made solely by automated means; and
- the kinds of decisions for which automated processing plays a substantial and direct role

You will have the right to request human intervention, express your point of view, and contest any such decision.

15. Personal Data breaches

If a data breach occurs involving personal information we hold, we will respond in accordance with our incident-response processes.

Where required by law, we will take reasonable steps to contain the breach and mitigate harm, conduct an assessment within 30 days (or as soon as practicable) and notify any affected individual and the Office of the Australian Information Commissioner (OAIC) if the breach is likely to result in serious harm from a personal information breach.

Where the GDPR applies, we will notify the relevant supervisory authority within 72 hours of becoming aware of a personal data breach, and will inform affected individuals without undue delay where the breach is likely to result in a high risk to their rights and freedoms.

16. Complaints

If you have a privacy complaint or concern, contact us at dataprotection@ssp-au.com (or write to the postal address above,). We will acknowledge and investigate your complaint and respond within a reasonable time. If we need more time, we will tell you why and keep you updated.

If you are not satisfied with our response, you may lodge a complaint with the relevant regulatory authority:

- Australia: Office of the Australian Information Commissioner (OAIC) – www.oaic.gov.au
- European Union: you may lodge a complaint with the supervisory authority in the EU Member State of your habitual residence, place of work or where the alleged infringement occurred.
- United Kingdom: Information Commissioner's Office (ICO)

17. Changes to this policy

We may update this Privacy Policy from time to time to reflect changes in our practices, systems or legal requirements. The current version will be published on our website and/or available on request.

Appendix A

Key Definitions/ Glossary

Adequacy Decision	Means a formal decision adopted by the European Commission or by the UK government determining that a non-EU or no-UK country, territory, specific sector or international organisation ensures an adequate level of protection for personal data, so that personal data can be transferred there without needing additional transfer safeguards such as SCCs.
APP Entity	means an organisation in Australia responsible for handling personal information under the Australian Privacy Principles (APPs) in the Privacy Act 1988.
Australian Privacy Principles (APPs)	Means the 13 principles under the Privacy Act 1988 (Cth) governing collection, use, disclosure, and management of personal information by APP Entity.
Biometric Information	Means data derived from physical or behavioural characteristics for identification, e.g. fingerprints or facial recognition templates.
Data Controller	Means the entity determining purposes and means of processing personal data.
Data Subject	An identified or identifiable living individual whose personal data is processed.
Legitimate Interests	Means a lawful basis for processing personal information where processing is necessary for the legitimate business interests of SSP Australia or a third party, provided that such interests are not overridden by your interests or fundamental rights and freedoms, as granted under applicable data protection laws (such as the GDPR).
Personal Information/ Personal Data	means any information or any opinion directly or indirectly relating to an identified individual, or an individual who is reasonably identifiable, whether the information or opinion is true or not, and whether recorded in material form or not.
Processing	Means any operation or set of operations performed on personal information or on sets of personal information, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure (including by transmission or otherwise making available), alignment or combination, restriction, erasure or destruction.
Sensitive Information/ Sensitive Data/	Means personal data that reveals or relates to any of the following types of information about an individual: • Health information (including physical or mental

Special Category Data	health) • Information about racial or ethnic origin • Political opinions or associations • Religious beliefs or affiliations • Philosophical beliefs • Sexual orientation or practices • Criminal record • Biometric information used for identification purposes (e.g. fingerprint) • Genetic data
Standard Contractual Clauses (SCCs)	