

AESION

PRIVACY POLICY

GLOBAL PERSONAL INFORMATION AND DATA PROTECTION NOTICE

Effective date: 27 July 2026

AESION operates across strategy, design, innovation, marketing and technology through a globally configured network. This Policy creates one clear privacy framework while recognising that responsibility follows the AESION entity and legal role involved in each Website, engagement and processing activity.

For www.aesion.co.nz, the primary Website Controller is AESION Creative Solutions New Zealand Limited. For a Client engagement, the Contracting Entity and the Controller or Processor roles are determined by the Order Documents and actual processing.

The AESION entity that determines the purpose and essential means of processing is responsible as Controller for that activity.

CONTENTS

PART A POLICY FRAMEWORK

Sections 1 to 5

PART B PERSONAL INFORMATION WE HANDLE

Sections 6 to 14

PART C COLLECTION AND USE

Sections 15 to 22

PART D DISCLOSURE AND GLOBAL PROCESSING

Sections 23 to 28

PART E DATA LIFECYCLE AND CHOICES

Sections 29 to 34

PART F RIGHTS AND REGIONAL NOTICES

Sections 35 to 40

PART G ADMINISTRATION AND CONTACT

Sections 41 to 43

Privacy responsibility follows the AESION entity and legal role involved in the relevant processing activity.

PART A. POLICY FRAMEWORK

1. SCOPE AND APPLICATION

- 1.1 This Privacy Policy explains how AESION collects, uses, holds, shares, transfers, retains and protects Personal Information in connection with AESION Websites, enquiries, business relationships, Services and global operations.
- 1.2 This Policy applies to Website visitors, prospective and current clients, client personnel, suppliers, professional partners, research participants, event and production participants, job applicants and other individuals who interact with AESION in a business or professional context.
- 1.3 This Policy does not govern a website, application, platform, product or system that AESION designs or develops for a Client but that the Client or another party operates. The privacy notice of that operator applies to its collection and use of Personal Information.
- 1.4 Where AESION processes Personal Information solely on a Client's documented instructions in providing Services, AESION generally acts as a Processor and the Client's privacy notice governs the relationship with the affected individuals. Section 3 explains this distinction.
- 1.5 This Policy does not apply to a third-party website, platform or service merely because a Website links to it, embeds it or enables a user to connect to it.
- 1.6 A service-specific, regional, participant, recruitment, workforce or just-in-time privacy notice may supplement this Policy. The more specific notice governs the processing activity it describes if there is an inconsistency.

2. PRIVACY RESPONSIBILITY AND CONTROLLER IDENTITY

- 2.1 For www.aesion.co.nz and any AESION Website that links to this Policy without identifying another operator, AESION Creative Solutions New Zealand Limited is the Website operator and primary Controller for Personal Information collected through that Website.
- 2.2 For a paid engagement, the AESION Contracting Entity identified in the applicable Order Document is generally the Controller of Personal Information it uses for relationship management, contracting, billing, security, compliance and its own business operations.
- 2.3 Another AESION entity may be the Controller for its own local recruitment, workforce, supplier, event or marketing activities. The relevant collection notice or communication will identify that entity where required.

- 2.4 Using personnel, affiliates, studios, contractors or professional partners in several countries does not by itself make every AESION entity a joint Controller. Responsibility under Privacy Laws follows the purposes, decisions and actual role of each participant.
- 2.5 Where two or more AESION entities jointly determine material purposes and means of processing, they will allocate privacy responsibilities as required by law. A summary of the arrangement will be made available where an individual is entitled to receive it.
- 2.6 The privacy contact method for the Website operator and other AESION Controllers is set out in section 43.

3. ROLES IN CLIENT ENGAGEMENTS

- 3.1 AESION acts as a Controller when it determines why and how Personal Information is used for its own engagement administration, financial management, quality assurance, security, legal compliance, service improvement and professional relationship purposes.
- 3.2 AESION acts as a Processor when it handles Personal Information on behalf of a Client and under the Client's documented instructions, such as when migrating a Client dataset, configuring a CRM, building a user database, operating a support environment or analysing Client-supplied audience data.
- 3.3 If an engagement requires a data processing agreement, security schedule or similar addendum, the parties must enter that document before the relevant processing begins. That document governs Processor activities and prevails over this Policy for its specific subject matter.
- 3.4 A Client remains responsible for its role as Controller, including the lawfulness of its instructions, collection notices, lawful bases, consents, data quality, retention requirements and responses to individuals, unless an Order Document expressly allocates a responsibility to AESION.
- 3.5 AESION may appoint service providers and specialist personnel as subprocessors where permitted by the Agreement. AESION will apply contractual, organisational and technical safeguards appropriate to the processing and any agreed data processing addendum.
- 3.6 AESION may create aggregated or de-identified information from engagement data where permitted by the Agreement and Privacy Laws. AESION will not intentionally re-identify properly anonymised information except to test the effectiveness of anonymisation or as otherwise permitted by law.

4. DEFINITIONS

- 4.1 AESION means the AESION entity that is the Controller or Processor for the processing activity in question.

- 4.2 AESION Group means any entity, studio, business unit or operating company that uses the AESION brand under common ownership, control or authorisation.
- 4.3 Client means the person or organisation that requests, receives or contracts for Services.
- 4.4 Contracting Entity means the AESION Group entity identified in the applicable Order Document. If no entity is expressly identified, it is the entity that accepts the engagement and issues the first invoice.
- 4.5 Controller means the person or organisation that determines the purposes and essential means of processing Personal Information. Equivalent terms under local law include business and personal information handler.
- 4.6 Order Document means a proposal, quotation, scope of work, statement of work, order form, service schedule, engagement letter or other written document that records an engagement.
- 4.7 Personal Information means information relating to an identified or reasonably identifiable individual. It includes personal data and similar concepts protected by applicable Privacy Laws.
- 4.8 Privacy Laws means privacy, data protection, electronic communications, direct marketing and related laws that apply to the relevant processing activity.
- 4.9 Processor means a person or organisation that processes Personal Information on behalf of and under the instructions of a Controller. Equivalent local terms include service provider, contractor and entrusted person.
- 4.10 Services means the strategy, research, design, innovation, marketing, digital, technology, software, IT, production, advisory and related services described in an Order Document.
- 4.11 Sensitive Information means Personal Information given enhanced protection under applicable law, including special-category data, health, biometric, genetic, precise geolocation, government identifier, financial credential, criminal history and children's information where protected.
- 4.12 Website means a website, portal, landing page or online service operated by or for AESION.

5. PRIVACY PRINCIPLES AND POLICY HIERARCHY

- 5.1 AESION aims to process Personal Information lawfully, fairly and transparently; for specified and legitimate purposes; in a proportionate and limited manner; accurately; only for as long as needed; and with safeguards appropriate to the risk.

- 5.2 The Privacy Laws that apply may depend on the Controller, the location and role of the processing, the location of the individual, the nature of the information and the way AESION offers or monitors Services. Mandatory legal rights and restrictions remain unaffected.
- 5.3 This Policy should be read with the AESION Terms and Conditions, applicable Cookie Settings, collection notices, Order Documents and any data processing or security addendum.
- 5.4 For privacy and security matters, a signed data processing or security addendum prevails for its specific subject matter, followed by the applicable Order Document, a specific collection notice and then this Policy, unless mandatory law requires another result.
- 5.5 Nothing in this Policy limits a right or remedy that cannot lawfully be limited. A statement that AESION may process information is subject to an applicable lawful basis, any required notice or consent, and the principle of necessity.
- 5.6 If AESION provides a translated version, the English version governs to the extent permitted by law unless a local notice states otherwise.

PART B. PERSONAL INFORMATION WE HANDLE

6. ENQUIRY AND RELATIONSHIP INFORMATION

- 6.1 When a person makes an enquiry, AESION may collect their name, job title, organisation, professional contact details, country or region, time zone, preferred language and relationship to the proposed engagement.
- 6.2 An enquiry may include an organisation's current Website, the engagement or service of interest, objectives, preferred timing, indicative investment, currency, existing materials, additional context and any files or links the person chooses to provide.
- 6.3 AESION may retain correspondence, meeting details, notes, proposals, decisions, feedback and a record of follow-up. A meeting may be recorded or transcribed only after an appropriate notice and, where required, consent.
- 6.4 If a person gives AESION information about another individual, the person should have authority to do so and should direct that individual to this Policy or another applicable notice.
- 6.5 A general enquiry form is not an approved channel for Sensitive Information, confidential source material, production credentials or regulated datasets. Such information should be provided only after AESION supplies an appropriate secure channel.

7. CLIENT AND PROJECT INFORMATION

- 7.1 AESION may collect the names, roles, contact details, authority levels, availability and communication preferences of Client stakeholders and other project participants.
- 7.2 Project information may include briefs, research inputs, stakeholder feedback, approvals, content, brand assets, account identifiers, test data, support requests, change records, meeting notes, deliverables and project history.
- 7.3 Where Services require access to a Client environment, AESION may process user identifiers, permissions, authentication records, audit events, system logs, device information and support diagnostics. Credentials should be shared through an approved secure method.
- 7.4 Depending on scope, a Client may provide datasets concerning its customers, users, employees, suppliers, research participants or other individuals. AESION will process that information in the role stated in the Agreement and only for authorised purposes.
- 7.5 Information about business strategy, performance, behaviour or opinions may be Personal Information when it identifies or can reasonably be linked to an individual, even if it is supplied in a professional context.

8. WEBSITE, DEVICE AND USAGE INFORMATION

- 8.1 When a person uses a Website, AESION and authorised providers may collect an internet protocol address, browser and device type, operating system, language, time zone, approximate location, referring address, page views, timestamps, interactions, downloads and error information.
- 8.2 A Website may use cookies, pixels, tags, software development kits, local storage, server logs and similar technologies to operate features, maintain security, remember choices, measure performance and, where permitted, support analytics or advertising.
- 8.3 AESION may record consent choices, security events, suspected bot or abuse signals, session information and diagnostic data needed to protect the Website and investigate technical issues.
- 8.4 AESION will not intentionally access precise location, a device camera, microphone, contacts or similar device permissions through a Service unless the individual activates a feature requiring that access and receives an appropriate permission request.
- 8.5 Further information about active technologies, providers, purposes and durations may be presented in the Website's Cookie Settings or cookie notice.

9. MARKETING AND COMMUNICATIONS INFORMATION

- 9.1 AESION may hold newsletter or event subscriptions, consent records, preferred topics, communication history, campaign source, delivery status, engagement with messages and opt-out choices.
- 9.2 For carefully targeted business communications, AESION may use professional role, organisation, industry, market, public business profile, prior interaction and an assessment of likely relevance.
- 9.3 Subject to law and user settings, marketing technologies may indicate whether a message was delivered, opened or selected. AESION uses that information to measure relevance, manage frequency and improve communications.
- 9.4 AESION does not purchase or use a marketing list without assessing its source, permitted use and notice requirements. A partner campaign or sponsored event may have an additional notice identifying the participating Controllers.

10. FINANCIAL AND TRANSACTION INFORMATION

- 10.1 AESION may collect billing contacts, billing addresses, purchase order information, tax or registration details, invoice history, payment status, expense records, bank account details for supplier payments and information needed to prevent fraud or resolve a dispute.

- 10.2 Payment card transactions are normally handled by a payment provider or financial institution. AESION generally receives confirmation, amount, currency, status and limited transaction references rather than a complete card number or security code.
- 10.3 Where proportionate and lawful, AESION may conduct business identity, sanctions, credit or fraud checks before extending payment terms or entering a higher-risk engagement.
- 10.4 Financial and transaction records may be retained for tax, accounting, audit, insurance, debt recovery and legal purposes as described in section 33.

11. RESEARCH, MEDIA AND PRODUCTION INFORMATION

- 11.1 Research, strategy and testing activities may involve survey responses, interview or workshop contributions, professional background, demographic information, opinions, preferences, usability behaviour, recordings, transcripts and incentive payment details.
- 11.2 Media, live, spatial and production Services may involve photographs, video, audio, appearance, voice, role, attendance, location information, talent arrangements and release or permission records.
- 11.3 Research may be anonymous, pseudonymous or identifiable. A participant notice, consent form, research protocol or Client notice will explain the particular arrangement and prevails for that activity.
- 11.4 AESION may use public sources, licensed databases, research panels, professional networks and Client-approved datasets where there is an appropriate basis. Public availability does not remove the need to use Personal Information fairly and lawfully.
- 11.5 AESION will ordinarily report research in aggregated or de-identified form unless identifiable reporting is necessary, expected in the context and authorised by the relevant Controller and participant notice.

12. RECRUITMENT, TEAM AND SUPPLIER INFORMATION

- 12.1 Recruitment information may include contact details, curriculum vitae, work history, education, portfolio, professional qualifications, work eligibility, references, interview notes, assessment results and remuneration expectations.
- 12.2 Information about employees, contractors and other team members is governed primarily by applicable workforce notices, contracts and local law. This Policy provides a general description where no more specific notice applies.
- 12.3 AESION may collect supplier and professional partner contact details, qualifications, availability, insurance, banking details, conflicts, sanctions information, performance records and due diligence materials.

- 12.4 Reference, background, identity or work eligibility checks will be conducted only where relevant, proportionate and permitted, with notice or consent where required.
- 12.5 An unsuccessful applicant's information is retained only for the recruitment cycle, a reasonable period for recordkeeping or claims, and any longer talent-pool period the applicant has accepted.

13. SENSITIVE AND REGULATED INFORMATION

- 13.1 AESION does not seek Sensitive Information as part of an ordinary Website enquiry or routine business relationship and will not intentionally collect it unless it is necessary for a defined and lawful purpose.
- 13.2 Sensitive Information may include health or disability information, race or ethnic origin, political or religious belief, trade union membership, sex life or sexual orientation, genetic or biometric identifiers, criminal history, precise geolocation, government identifiers, financial credentials and information about children.
- 13.3 Where AESION is authorised to handle Sensitive Information, it will use an additional legal condition, explicit or separate consent where required, restricted access and safeguards appropriate to the risk.
- 13.4 A Client must not provide Sensitive Information or ask AESION to collect it unless the applicable Order Document and, where required, data processing or security addendum expressly permit the processing.
- 13.5 If AESION receives Sensitive Information unexpectedly, it may securely delete, return, isolate or restrict it while determining the lawful and appropriate response.

14. CHILDREN AND MINORS

- 14.1 AESION Websites and ordinary Services are designed for businesses and professional users and are not directed to children.
- 14.2 AESION does not knowingly collect Personal Information directly from a child below 16, or a lower local age of digital consent where lawful, through a general Website. In mainland China, AESION treats information about a child under 14 as Sensitive Information. AESION will not knowingly use children's Personal Information for behavioural advertising, data brokerage or unrelated profiling.
- 14.3 A project involving children requires an express scope, a child-appropriate notice, a lawful basis, any required parent or guardian authorisation and safeguards proportionate to the child's age, capacity and risk.
- 14.4 A parent or guardian who believes a child has provided Personal Information without appropriate authorisation may submit a Privacy Request. AESION will investigate and delete or otherwise address the information where required.

PART C. COLLECTION AND USE

15. SOURCES AND METHODS OF COLLECTION

- 15.1 AESION collects Personal Information directly when a person submits a form, communicates with AESION, attends a meeting or event, participates in research, uses a Service, applies for a role, supplies work or enters a business relationship.
- 15.2 AESION may receive information indirectly from a Client, employer, colleague, representative, referral source, research panel, event organiser, supplier, professional adviser, platform, public company record, professional network or other lawful public source.
- 15.3 Where required, AESION will notify an individual of indirect collection within the applicable period. This includes obligations arising from New Zealand Information Privacy Principle 3A and equivalent transparency rules.
- 15.4 Technical information may be collected automatically from a device, browser, Website, application, network or integrated platform as described in sections 8 and 29.
- 15.5 AESION may combine information from several sources when the combined use is compatible with the original purposes, reasonably expected or covered by a new notice and lawful basis.
- 15.6 AESION will not treat public availability as blanket permission to scrape, compile, profile or republish Personal Information without regard to necessity, fairness and applicable restrictions.

16. ENQUIRIES AND PRE-CONTRACT STEPS

- 16.1 AESION uses enquiry information to respond, understand the opportunity, assess fit and availability, allocate an appropriate regional or specialist team, arrange discussions and prepare a proposal or other Order Document.
- 16.2 AESION may verify a person's authority, organisation and contact details; assess conflicts, sanctions, fraud, security or reputational risk; and retain a record of the decision to accept or decline an opportunity.
- 16.3 The usual lawful bases are taking steps requested before a contract, performing a contract, AESION's legitimate interests in developing and protecting professional relationships, consent where required, and compliance with legal obligations.
- 16.4 A person is not required to provide optional information. If required fields or information reasonably needed to assess an engagement are not provided, AESION may be unable to respond fully, prepare a reliable proposal or accept the engagement.

- 16.5 An enquiry may be shared within the AESION Group and with authorised specialists only to the extent reasonably needed to assess or respond to it.

17. DELIVERING AND MANAGING SERVICES

- 17.1 AESION uses Personal Information to establish an engagement, configure a team, manage access and permissions, plan and perform Services, communicate, review work, obtain approvals, test Deliverables and provide agreed support.
- 17.2 AESION may use relationship and project records for scheduling, resource management, quality assurance, invoicing, expense management, change control, service reporting and resolution of complaints or disputes.
- 17.3 AESION may verify that instructions and approvals come from an authorised person and may retain an audit record where this is important to security, scope, acceptance or legal rights.
- 17.4 When processing Client Personal Information as a Processor, AESION will follow the Agreement, the Client's documented lawful instructions and applicable data processing obligations.
- 17.5 A meeting, research session or support interaction may be recorded or transcribed only where appropriate notice is given and any required consent or other lawful basis is in place.

18. RESEARCH, MARKETING, DIGITAL AND TECHNOLOGY SERVICES

- 18.1 Market research, analysis and strategy Services may require stakeholder, audience, competitor, participant or behavioural information to identify needs, patterns, opportunities and risks.
- 18.2 Brand, creative, content, media, live, spatial and physical product Services may involve contributors, talent, production participants, permissions, audience testing and feedback needed to create, validate and publish work.
- 18.3 Digital marketing Services may involve CRM records, campaign audiences, consent signals, platform identifiers, conversion data, analytics and performance information. The Agreement must identify whether AESION acts as a Controller, Processor or authorised platform user for each material activity.
- 18.4 Website, application, ecommerce and digital product Services may involve user accounts, form submissions, test participants, session events, support records, transactions and technical logs. The operator of the deployed service is responsible for its end-user notice unless AESION is expressly appointed to operate it.
- 18.5 Software, automation, CRM, systems integration, SaaS, hosting coordination, IT infrastructure and digital transformation Services may involve migration, mapping,

testing, synchronisation, support, security and operational logs across connected environments.

- 18.6 The Order Document and any data processing or security addendum determine the permitted data, purposes, systems, locations, access, retention and responsibilities for a specific engagement.

19. BUSINESS OPERATIONS, COMPLIANCE AND PROTECTION

- 19.1 AESION uses Personal Information for accounting, tax, insurance, audit, procurement, supplier management, business planning, workforce allocation, governance and internal reporting.
- 19.2 AESION may process information to negotiate and enforce agreements, manage conflicts of interest, protect intellectual property, resolve complaints, collect debts and establish, exercise or defend legal claims.
- 19.3 AESION may monitor systems and communications metadata to maintain security, prevent fraud and misuse, investigate incidents, protect personnel and preserve evidence.
- 19.4 AESION may respond to a valid request from a court, regulator, law enforcement body or other authority. AESION will assess the request and disclose only information it reasonably believes is required or lawfully permitted.
- 19.5 Where necessary to protect life, safety, systems, rights or property, AESION may use or disclose information under an applicable emergency, vital interests or permitted-situation basis.

20. ANALYTICS, IMPROVEMENT AND DE-IDENTIFICATION

- 20.1 AESION may analyse Website performance, enquiry patterns, service delivery, project outcomes, support trends, campaign effectiveness and operational metrics to improve quality, usability, security and resource planning.
- 20.2 AESION may use appropriately limited project knowledge to improve its methods, templates, workflows and professional capabilities, but it will not disclose Client Confidential Information or identifiable Client results without authority.
- 20.3 Where practical, AESION uses aggregated, pseudonymised, synthetic or de-identified information for analytics, testing, benchmarking and service improvement.
- 20.4 Information is treated as anonymous only when it is not reasonably capable of identifying an individual under applicable law. Pseudonymised information remains Personal Information when it can be linked back using additional information.

- 20.5 AESION will not intentionally re-identify anonymous information except to validate de-identification, investigate security or comply with law, and then only with appropriate controls.

21. AI-ASSISTED AND AUTOMATED TOOLS

- 21.1 AESION may use AI-assisted, algorithmic and automated tools in research, ideation, design exploration, content development, coding, testing, analysis, optimisation, quality assurance, transcription and administration, subject to professional oversight and the agreed scope.
- 21.2 AESION will apply reasonable data minimisation, access, vendor and configuration controls. Unless authorised in writing with an appropriate lawful basis and safeguards, AESION will not submit Client Confidential Information or identifiable Client Personal Information to a public tool in a manner that permits the provider to use it for general model training.
- 21.3 An AI or automation provider may process limited Personal Information as an authorised service provider or subprocessor. Such use is subject to section 24, section 27 and any applicable data processing addendum.
- 21.4 AI-assisted processing may generate classifications, summaries, predictions or other inferences. AESION will use a level of human review reasonably appropriate to the purpose, accuracy needs and potential impact.
- 21.5 AESION does not use solely automated processing to make a decision about a Website visitor, applicant, Client contact or supplier that produces legal or similarly significant effects, unless a specific notice explains the decision, lawful basis, logic, consequences and available safeguards.
- 21.6 Automated spam filtering, malware detection, access logging, scheduling, analytics and similar operational tools may be used where they do not make a legally or similarly significant decision about an individual.

22. LAWFUL BASES AND REQUIRED INFORMATION

- 22.1 Where a law requires AESION to identify a lawful basis, AESION may rely on consent; steps requested before a contract; performance of a contract; compliance with a legal obligation; protection of vital interests; a task in the public interest where applicable; or legitimate interests that are not overridden by an individual's rights. Relevant legitimate interests may include responding to enquiries, delivering and improving Services, maintaining business relationships, allocating global resources, securing systems, preventing misuse, recovering amounts due, managing suppliers and protecting legal rights.

- 22.2 For direct marketing, cookies, Sensitive Information, children, international transfers and other higher-risk processing, AESION will use any additional consent, condition, assessment or safeguard required by law. Where consent is the basis, it must be freely given, specific, informed and unambiguous and may be withdrawn without affecting processing already lawfully carried out.
- 22.3 Some information is necessary to enter or perform a contract, verify authority, provide secure access, make payment, comply with law or respond to a rights request. Failure to provide it may prevent AESION from taking the requested action. Legal terminology and available bases differ by jurisdiction, so AESION applies the basis and conditions required for the particular Controller and activity.

PART D. DISCLOSURE AND GLOBAL PROCESSING

23. AESION GROUP AND GLOBAL TEAMS

- 23.1 AESION may share Personal Information with AESION Group entities, employees, contractors, specialist studios and authorised professional partners when reasonably needed to assess an enquiry, configure a team, deliver Services, maintain quality, administer the relationship, protect security or comply with law.
- 23.2 Access is intended to be role-based and limited to people who need the information for an authorised purpose. AESION applies confidentiality, data protection and security obligations appropriate to the recipient's role.
- 23.3 The AESION Group may coordinate administration, technology, finance, risk, procurement, communications and professional resources across regions. A transfer within the group remains subject to applicable purpose, necessity and cross-border rules.
- 23.4 A recipient AESION entity may act as a Processor, subprocessor, independent Controller or joint Controller depending on its decisions and responsibilities. Participation in delivery does not automatically make every AESION entity a party to the Client's contract or a Controller of all related information.
- 23.5 AESION does not provide every member of a global team with unrestricted access to a central record merely because the person works under the AESION brand.

24. SERVICE PROVIDERS, PARTNERS AND ADVISERS

- 24.1 AESION may use providers of Website hosting, cloud storage, collaboration, email, CRM, project management, design review, analytics, advertising, payment, accounting, research panels, transcription, production, recruitment, identity verification, IT, cybersecurity, backup and AI-assisted tools.
- 24.2 AESION may also disclose information to lawyers, accountants, auditors, insurers, banks, consultants and other professional advisers where reasonably necessary for their services.
- 24.3 AESION selects and manages providers using a level of due diligence and contractual protection appropriate to the service, information, location and risk. Providers acting for AESION are expected to process information only for authorised purposes.
- 24.4 Some providers, such as payment networks, social platforms, app stores, telecommunications providers and professional advisers, may act as independent Controllers under their own legal duties and notices.

- 24.5 Where a Client data processing addendum requires notice, authorisation or a list of subprocessors, AESION will follow that addendum. A current provider or subprocessor description may also be made available on reasonable request where required by law.

25. CLIENT-DIRECTED TOOLS AND THIRD-PARTY PLATFORMS

- 25.1 A Client may instruct AESION to access, configure or connect a third-party platform, account or integration. The Client is responsible for confirming that the instruction, account permissions and transfer are lawful and consistent with the platform terms.
- 25.2 Advertising networks, analytics tools, social media, payment providers, app stores, marketplaces, hosting services and other platforms may collect and use information as independent Controllers under their own notices.
- 25.3 Where AESION receives an access token, credential or delegated permission, AESION will use it only for the authorised engagement, apply reasonable security and remove or return access when it is no longer needed or when the Client instructs.
- 25.4 AESION is not responsible for a third party's independent processing, retention, security or policy. AESION will, however, use reasonable care in selecting or configuring a provider where that responsibility forms part of the Services.
- 25.5 If a Client requires a particular provider after AESION identifies a material privacy or security concern, the parties should record the instruction, allocation of risk and any additional safeguard in the Order Document.

26. CORPORATE, LEGAL AND REGULATORY DISCLOSURES

- 26.1 AESION may disclose Personal Information to a court, regulator, law enforcement body, tax authority or other public authority where disclosure is required or lawfully permitted.
- 26.2 AESION may share information with professional advisers, insurers, financiers and auditors to obtain advice, manage risk, establish or defend claims, complete audits or meet legal and contractual duties.
- 26.3 If an AESION business, entity or material asset is considered for investment, financing, reorganisation, merger, acquisition or sale, relevant information may be disclosed under confidentiality and due diligence safeguards. The receiving party may continue processing only as permitted by law and any applicable notice.
- 26.4 AESION may disclose information where reasonably necessary to protect the safety, rights, property or systems of AESION, a Client, an individual or the public, including to investigate fraud, cyber incidents, misuse or unlawful activity.
- 26.5 Where legally permitted and appropriate, AESION will seek to notify the affected Controller or individual before a compulsory disclosure and will challenge or narrow a request it reasonably considers excessive or invalid.

27. INTERNATIONAL TRANSFERS AND SAFEGUARDS

- 27.1 AESION's globally configured delivery model means Personal Information may be accessed, hosted, supported or processed outside the country in which it was collected.
- 27.2 Before an international transfer, AESION will use the mechanism required by applicable law. Depending on the transfer, this may include an adequacy decision, standard contractual clauses, the United Kingdom International Data Transfer Agreement or Addendum, a binding agreement, certification, security assessment, regulator-approved mechanism, consent or a permitted derogation.
- 27.3 AESION may conduct transfer and vendor risk assessments and adopt measures such as access limitation, encryption, data minimisation, regional hosting, contractual controls and documented instructions where proportionate.
- 27.4 For transfers from mainland China, AESION will implement any required security assessment, standard contract, certification, personal information protection impact assessment, separate consent, localisation or recipient notice before the transfer.
- 27.5 For transfers governed by New Zealand or Australian law, AESION will take the steps required to ensure an overseas recipient is subject to comparable protection or that another lawful exception applies, including accountability measures where required.
- 27.6 An individual may request information about a transfer safeguard that applies to their Personal Information. AESION may provide a summary or redacted copy where necessary to protect confidentiality, security and the rights of others.

28. OVERSEAS LOCATIONS AND ACCESS

- 28.1 Countries in which AESION personnel, group entities or material service providers are likely to process or access Personal Information may include Australia, China, Germany and other countries in the European Economic Area, New Zealand, the United Kingdom and the United States.
- 28.2 Information may also be processed in the country of a Client, research participant, specialist provider, production partner or project team where that location is necessary for the engagement.
- 28.3 Not every category of Personal Information is transferred to every listed country. The recipient, location and information depend on the Website, Client, Service, provider configuration and delivery team.
- 28.4 Cloud and platform providers may use distributed infrastructure, support locations and resilience regions that change over time. AESION will identify specific locations in a data processing addendum or collection notice where required or materially relevant.
- 28.5 Remote access from another country may constitute an international transfer under some Privacy Laws and will be treated accordingly.

PART E. DATA LIFECYCLE AND CHOICES

29. COOKIES AND SIMILAR TECHNOLOGIES

- 29.1 A Website may use strictly necessary technologies for security, network management, consent records, load balancing, accessibility, session continuity and features requested by the user.
- 29.2 With consent where required, a Website may use functional, analytics, performance, advertising or social media technologies to remember choices, understand use, measure campaigns and present relevant communications.
- 29.3 AESION will not activate non-essential cookies or similar technologies before valid consent where applicable law requires prior consent. Rejecting non-essential technologies should remain available without preventing access to ordinary Website content.
- 29.4 A user may manage choices through the Cookie Settings, withdraw consent, clear browser storage or adjust browser controls. Some requested functions may not operate correctly if necessary storage is blocked.
- 29.5 AESION will respect a valid browser-based opt-out preference signal, including Global Privacy Control, to the extent required by applicable law and supported by the relevant Website configuration.
- 29.6 The Cookie Settings or cookie notice may identify current providers, cookie names, purposes and durations. If there is a conflict about a specific technology, that more detailed notice governs.

30. DIRECT MARKETING AND COMMUNICATION PREFERENCES

- 30.1 AESION may send service, security, legal, transaction and project communications that are necessary for an enquiry or business relationship. These are not marketing messages and may continue after a marketing opt-out where still required.
- 30.2 Marketing consent is optional and separate from acknowledgement of this Policy. Where consent is required, AESION will not treat submission of a general enquiry as consent to unrelated promotional communications.
- 30.3 Where permitted for professional business communications, AESION may rely on a relevant existing relationship or a balanced legitimate interest, provided the message is proportionate, identifies AESION and offers an effective opt-out.
- 30.4 A person may unsubscribe through the message or submit a Privacy Request. AESION will stop the affected direct marketing within the period required by law.

- 30.5 AESION may retain minimal contact information on a suppression list to ensure an opt-out is respected. A suppression record is not used to resume marketing.
- 30.6 AESION does not knowingly direct marketing to children. Refusing or withdrawing marketing consent does not reduce access to an ordinary enquiry process or contracted Service.

31. SECURITY AND ACCESS CONTROLS

- 31.1 AESION maintains risk-based administrative, organisational and technical safeguards designed to protect Personal Information against accidental or unlawful loss, misuse, alteration, destruction, access and disclosure.
- 31.2 Measures may include role-based access, authentication, least-privilege controls, encryption in transit and at rest where appropriate, secure configuration, logging, backups, confidentiality obligations, workforce awareness, vendor assessment and incident response procedures.
- 31.3 Security measures are selected according to the nature, volume, context and sensitivity of the information; available technology; implementation cost; and the likelihood and severity of harm.
- 31.4 No transmission, storage system or security measure can be guaranteed completely secure, uninterrupted or immune from attack. AESION therefore reviews safeguards and adapts them as risks, Services and technology change.
- 31.5 A user must protect their credentials, use authorised channels and promptly notify AESION of suspected compromise. A Client remains responsible for security controls assigned to it under the Agreement and for changes made outside AESION's control.
- 31.6 AESION does not publish security details that would materially weaken a safeguard. Additional security information may be provided under confidentiality during a suitable procurement or risk review.

32. PERSONAL DATA BREACHES

- 32.1 AESION maintains processes to assess, contain, investigate, document and remediate a suspected or confirmed breach affecting Personal Information.
- 32.2 Where AESION acts as a Controller, it will notify affected individuals and competent regulators when and within the period required by applicable Privacy Laws.
- 32.3 Where AESION acts as a Processor, it will notify the relevant Client without undue delay after becoming aware of a confirmed Personal Information breach, provide reasonably available information and support the Client's response as required by the Agreement and law.

- 32.4 A notice may describe the nature of the incident, categories of information and people affected, likely consequences, measures taken and recommended protective steps, subject to security, legal and investigative restrictions.
- 32.5 A person who suspects unauthorised access, disclosure or misuse involving AESION should submit a Privacy Request promptly and should not include passwords or unnecessary Sensitive Information in the initial report.

33. RETENTION, ARCHIVING AND DELETION

- 33.1 AESION retains Personal Information only for as long as reasonably needed for the purpose collected, an approved compatible purpose, the Agreement, a legal or regulatory duty, security, audit, insurance, dispute resolution or establishment and defence of claims.
- 33.2 Retention criteria include the status and duration of the relationship, sensitivity and volume, operational need, expected follow-up, contractual commitments, statutory recordkeeping, limitation periods, unresolved complaints, security risk and whether the information can be safely de-identified.
- 33.3 Enquiry and prospect records are reviewed after the opportunity becomes inactive. Contract, invoice, tax and transaction records are retained for applicable statutory and audit periods. Project information is retained through delivery and a reasonable handover, support and claims period unless an Order Document sets another period.
- 33.4 Marketing records are retained while the relationship or permission remains relevant, subject to periodic review. Suppression information may be retained longer to preserve an opt-out. Recruitment records are retained for the hiring cycle and a reasonable legal or agreed talent-pool period.
- 33.5 Client Personal Information processed as a Processor will be returned, deleted, anonymised or retained according to the data processing addendum, Client instruction and mandatory law. AESION is not an archival service unless an Order Document expressly includes archival retention.
- 33.6 Deletion from active systems may be followed by expiry from protected backups according to established cycles. AESION may isolate information under legal hold and restrict it to the purpose requiring continued retention.

34. ACCURACY, MINIMISATION AND ANONYMISATION

- 34.1 AESION takes reasonable steps to keep Personal Information accurate, current and limited to what is necessary. Individuals and Clients should promptly provide corrections. Where practical, AESION uses synthetic, masked, aggregated or de-identified information and deletes obsolete or inaccurate records, subject to legal retention. Privacy rights may cease once information is truly anonymised.

PART F. RIGHTS AND REGIONAL NOTICES

35. GENERAL PRIVACY RIGHTS

- 35.1 Depending on applicable law, an individual may have rights to know whether AESION processes their Personal Information; access or receive a copy; correct it; delete it; restrict processing; object; withdraw consent; obtain portability; or complain.
- 35.2 An individual may also have rights to opt out of direct marketing, sale, sharing, targeted advertising or certain profiling; limit use of Sensitive Information; receive information about international transfer safeguards; or appeal a refusal.
- 35.3 Rights are not absolute. AESION may retain or withhold information where an exemption applies, including legal privilege, security, fraud prevention, recordkeeping, legal claims, disproportionate impact on others or inability to verify the requester.
- 35.4 AESION will not discriminate against a person for exercising a privacy right. AESION does not ordinarily charge a fee, but may charge or decline a manifestly unfounded, excessive or repetitive request where law permits.
- 35.5 Where AESION acts only as a Processor, it may refer the request to the relevant Client and provide reasonable assistance. The Client remains responsible for the response unless the Agreement or law states otherwise.
- 35.6 Rights concerning deceased persons, authorised representatives or household data apply only where recognised by the relevant jurisdiction.

36. EUROPEAN ECONOMIC AREA AND UNITED KINGDOM

- 36.1 Where the EU GDPR or United Kingdom GDPR applies, the Controller and any required representative will be identified in this Policy, the relevant collection notice or the applicable Order Document. AESION will identify a data protection officer only where one is appointed or legally required.
- 36.2 Individuals may have rights of access, rectification, erasure, restriction, portability, objection and withdrawal of consent, together with a right not to be subject to a solely automated decision producing legal or similarly significant effects.
- 36.3 An objection to processing for direct marketing will be honoured. An objection to processing based on legitimate interests will be assessed against any compelling legitimate grounds and the need to establish, exercise or defend legal claims.
- 36.4 Transfers outside the European Economic Area or United Kingdom will use an adequacy decision, approved contractual mechanism or another lawful safeguard as described in section 27.

- 36.5 An individual may complain to the supervisory authority in the country where they live or work, where the alleged issue occurred, or to the United Kingdom Information Commissioner's Office where applicable.
- 36.6 AESION will respond within the period required by applicable law and will inform the requester of any lawful extension, refusal and available complaint route.

37. NEW ZEALAND AND AUSTRALIA

- 37.1 Where the New Zealand Privacy Act 2020 applies, AESION will follow the Information Privacy Principles, including the collection notice requirements for directly and indirectly collected information, rights of access and correction, retention limits and safeguards for overseas disclosure.
- 37.2 A person may request access to or correction of Personal Information and may submit a complaint to the Office of the Privacy Commissioner if dissatisfied with AESION's response.
- 37.3 Where the Australian Privacy Act 1988 and Australian Privacy Principles apply, this Policy is intended to describe the kinds of information handled, methods and purposes, access and correction process, complaint process and likely overseas locations.
- 37.4 An Australian privacy complaint will be acknowledged, assessed by an appropriate person, investigated using reasonably available information and answered within a reasonable period. AESION may ask for further details and will explain the outcome and available escalation route.
- 37.5 An Australian individual may complain to the Office of the Australian Information Commissioner after giving AESION a reasonable opportunity to address the issue.
- 37.6 AESION will assess and notify eligible data breaches under the applicable New Zealand or Australian notification regime.

38. MAINLAND CHINA

- 38.1 Where the Personal Information Protection Law of the People's Republic of China applies, the relevant AESION entity acts as the personal information handler for processing it determines and will provide the required information about purposes, methods, categories, retention and rights.
- 38.2 AESION will obtain consent, separate consent or written consent where required, including for Sensitive Personal Information, provision to another handler, public disclosure and cross-border provision.
- 38.3 Sensitive Personal Information is processed only where necessary for a specific purpose, with enhanced safeguards. Information about a child under 14 requires parent or guardian consent and child-specific protections.

- 38.4 A transfer from mainland China will use the lawful cross-border mechanism and notices described in section 27. Where required, AESION will identify the overseas recipient, contact details, purpose, method, information categories and means for exercising rights.
- 38.5 Individuals may have rights to know, decide, restrict or refuse processing; access and copy; correct or complete; delete; withdraw consent; request an explanation of processing rules; and exercise rights recognised for a deceased close relative.
- 38.6 If local law requires a representative, dedicated institution, security assessment, filing or data localisation arrangement, the relevant AESION operation will implement and identify it in a local notice before the affected processing.

39. UNITED STATES

- 39.1 If a United States state privacy law applies, the categories AESION may have collected during the preceding 12 months are described in sections 6 to 13. They may include identifiers, professional and commercial information, internet or network activity, approximate geolocation, audio or visual information, employment information, inferences and limited Sensitive Information where necessary.
- 39.2 Sources are described in section 15; business and commercial purposes are described in sections 16 to 22; and categories of recipients are described in sections 23 to 26. AESION does not collect every category for every person.
- 39.3 AESION does not sell Personal Information for monetary consideration. Depending on the configuration of non-essential analytics or advertising technologies, a disclosure may be defined as sale, sharing or targeted advertising under a particular state law. Where that law applies, AESION will provide the required privacy choice and honour a valid opt-out preference signal.
- 39.4 AESION does not knowingly sell or share the Personal Information of children and does not use or disclose Sensitive Information beyond purposes permitted without a separate right to limit unless an appropriate notice and choice are provided.
- 39.5 Applicable rights may include confirmation, access, correction, deletion, portability, opt-out of sale, sharing, targeted advertising or qualifying profiling, limitation of Sensitive Information, appeal and freedom from discrimination.
- 39.6 AESION does not offer a financial incentive for Personal Information unless a separate notice describes the material terms, value calculation and right to withdraw.

40. REQUESTS, VERIFICATION AND COMPLAINTS

- 40.1 A person may exercise a right or make a complaint by submitting a Privacy Request through the method in section 43. The request should identify the relevant relationship, Website, project or communication and the right or concern involved.
- 40.2 AESION may request information reasonably necessary to verify identity, authority and scope. Verification will be proportionate to the sensitivity of the information and the risk of unauthorised disclosure.
- 40.3 An authorised agent may submit a request where permitted. AESION may require evidence of authority and may verify identity directly with the individual unless law provides otherwise.
- 40.4 AESION will acknowledge and investigate a complaint, involve the responsible Controller or Client where appropriate, keep a reasonable record and respond within the period required by applicable law.
- 40.5 If AESION refuses or limits a request, it will explain the reason and available appeal or complaint route to the extent required and legally permitted.
- 40.6 A person may complain to a competent privacy or data protection regulator. AESION encourages the person to contact AESION first so it has an opportunity to address the issue, but doing so does not limit a statutory right to approach a regulator directly.

PART G. ADMINISTRATION AND CONTACT

41. THIRD-PARTY SITES AND CLIENT-CONTROLLED SERVICES

- 41.1 A Website may contain links to, content from or sign-in options provided by third parties. Their privacy practices are governed by their own notices, and AESION is not the Controller of their independent processing.
- 41.2 A Client-controlled website, application, ecommerce service, CRM, portal or software environment developed or supported by AESION remains subject to the Client's privacy notice unless an express written arrangement appoints an AESION entity as operator or Controller.
- 41.3 Messages sent through a social media or marketplace account may be processed both by AESION and the platform. Users should avoid posting confidential or Sensitive Information in public or unsecured channels.
- 41.4 If a user authorises a third-party login or integration, the information shared depends on the user's settings and the third party's permission screen. The user may be able to revoke access through that third party.
- 41.5 A link or integration does not imply that AESION endorses the third party's privacy, security or content practices.

42. CHANGES TO THIS POLICY

- 42.1 AESION may update this Policy to reflect changes in law, Services, technology, providers, global operations or privacy practices.
- 42.2 The current version will display its effective date. AESION will provide additional notice of a material change where required or where the change would not reasonably be expected in the context.
- 42.3 AESION will not use previously collected Personal Information for a materially incompatible new purpose without a lawful basis and any notice or consent required at that time.
- 42.4 A previous version may be retained for governance and dispute purposes and may be made available on reasonable request.
- 42.5 A change to this Policy does not override a signed data processing addendum, Order Document or mandatory legal requirement.

43. PRIVACY CONTACT AND WEBSITE OPERATOR

- 43.1 For www.aesion.co.nz and any AESION Website that links to this Policy without naming another operator, the Website operator and primary privacy Controller is AESION Creative Solutions New Zealand Limited.

- 43.2 To make a privacy enquiry, rights request, complaint or security report, use the enquiry form on www.aesion.co.nz and write Privacy Request at the beginning of the Additional Context field. Do not include passwords or unnecessary Sensitive Information in the initial submission.
- 43.3 For a paid engagement, a person may also contact the AESION Contracting Entity through the project contact or notice channel stated in the applicable Order Document or invoice.
- 43.4 If a local representative, data protection officer or privacy officer is required for a specific processing activity, the relevant collection notice or regional legal notice will provide that person's or organisation's contact details.
- 43.5 AESION will use information submitted in a Privacy Request only to verify, investigate, respond, maintain an appropriate record and comply with law.
- 43.6 Submitting a privacy concern through AESION does not prevent an individual from contacting a competent regulator or exercising any other right available under applicable law.