



PRIVACY POLICY

Data handling, security and data-breach management

Global Psychosocial Safety Network Pty Ltd
trading as Humn IQ®
Suite 44, Marnirni-apinthe Building, Lot Fourteen, North Terrace, Adelaide SA 5000

HIQ-LGL-003 | Version 1.2

Commercial in Confidence

1. Introduction

1.1 At Humn IQ®, trust is fundamental to everything we do. Organisations entrust us with information about their people, their workplaces and the psychosocial risks that influence health, safety and wellbeing. We recognise that this information may be sensitive and that protecting it is essential to maintaining the confidence of our customers, survey participants and partners.

1.2 This Privacy Policy explains how Global Psychosocial Safety Network Pty Ltd (trading as Humn IQ®) (**Humn, we, us**) collects, uses, stores, protects and discloses personal information when you use our website, software platform and related services. It also explains how we use de-identified and aggregated information to improve the Platform, develop industry benchmarking and support research into healthier workplaces.

1.3 This Privacy Policy also sets out Humn's data-processing commitments to customers, including the respective responsibilities of the parties, permitted processing activities, use of sub-processors, international processing, information security, data retention, data-breach management and the return or deletion of Customer Data. For customers, this Privacy Policy forms part of the Contract and is to be read together with the Platform Subscription Agreement, the Platform Terms & Conditions and the Information Security Schedule (Schedule 3). Where there is any inconsistency, the order of precedence in clause 1.4 of the Platform Subscription Agreement applies.

2. About Humn IQ®

2.1 Humn IQ® is a cloud-based psychosocial risk intelligence platform. It assists organisations to identify psychosocial hazards, understand emerging workplace risks, support consultation with workers and inform evidence-based risk management. It provides technology and reporting tools to support organisational decision-making, and does not replace professional judgement, legal advice, clinical assessment or an organisation's obligations under work health and safety legislation.

2.2 Depending on how the Platform is used, Humn may collect information directly from you, process information on behalf of a customer, or process de-identified information to improve the Platform.

2.3 Humn does not sell identifiable personal information or survey responses, does not disclose identifiable benchmarking information, does not make automated employment decisions, and does not replace organisational consultation. Before information is used for benchmarking, Humn applies technical and organisational measures, including minimum reporting thresholds, designed to minimise the likelihood that an individual or organisation could reasonably be identified.

3. Scope

3.1 This Privacy Policy applies to visitors to our website; organisations using the Platform; individuals who complete surveys using the Platform; Authorised Users; prospective customers; individuals who contact Humn; participants in demonstrations, webinars or events; and users of related Humn services. It applies whether information is collected directly by Humn or through organisations using the Platform.

4. Our privacy commitment

4.1 Humn is committed to handling information responsibly. Our privacy practices are guided by five principles: **respect** (we treat personal information with care); **transparency** (we explain how information is collected and

used); **security** (we apply controls designed to protect information throughout its lifecycle); **minimisation** (we collect only the information reasonably necessary to provide our services); and **continuous improvement** (we review our practices to reflect changes in technology, legislation and expectations).

5. Compliance

5.1 Humn seeks to comply with the *Privacy Act 1988* (Cth), the Australian Privacy Principles (APPs), other applicable Australian privacy legislation, and the contractual privacy obligations agreed with customers. Where a customer contract requires additional privacy or security controls, those contractual obligations also apply.

5.2 Humn processes Customer Data in accordance with the principles of lawfulness, transparency, confidentiality, integrity, accountability, data minimisation, privacy by design, security by default and continuous improvement. These principles underpin the design, operation and ongoing development of the Platform.

5.3 Humn maintains an information security management system (ISMS) that is being developed to align with ISO/IEC 27001, the NIST Cybersecurity Framework 2.0 and the ASD Essential Eight (Maturity Level One), which supports Humn's handling of personal information. Humn does not claim formal certification against a framework unless and until the relevant requirements have been assessed and evidenced.

6. Definitions

For this Policy:

Aggregated Data means information combined from multiple organisations or individuals in a manner that does not reasonably identify any person or organisation.

Benchmark Data means aggregated and appropriately de-identified information derived from Customer Data and Survey Data that does not reasonably identify an individual or a participating organisation.

Customer means the organisation that subscribes to the Platform.

Customer Data means all information uploaded or entered into the Platform by or on behalf of a Customer.

De-identified Data means information that has been processed so that individuals are not reasonably identifiable.

Personal Information has the meaning given in the *Privacy Act 1988* (Cth): information or an opinion about an identified individual, or an individual who is reasonably identifiable.

Platform means the Humn IQ® software, websites, applications and related services.

Platform Data means operational information generated through the use of the Platform.

Respondent means an individual completing a survey through the Platform.

Sensitive Information has the meaning given in the *Privacy Act 1988* (Cth) and includes information about an individual's health and other categories protected under Australian privacy law. In the context of the Platform, Sensitive Information may include information relating to psychological wellbeing, mental health, workplace behaviours, bullying, harassment, discrimination, occupational stress or exposure to traumatic events, where that information is about an identifiable individual.

Survey Data means information collected through assessments, surveys or questionnaires administered using the Platform.

7. How we classify information

The Platform processes different categories of information depending on how it is used.

Personal Information: information about an identifiable individual, for example name, work email address, telephone number, position title and account details.

Customer Data: all information provided to the Platform by, or on behalf of, a Customer, which may include organisational information, user accounts, survey configuration, demographic settings, uploaded documents, action plans, risk registers, implementation information and survey responses. Unless otherwise agreed in writing, Customers retain ownership of their Customer Data.

Survey Data: information collected through assessments, surveys or questionnaires, which may include psychosocial hazard responses, leadership perceptions, work-design information, wellbeing indicators, consultation feedback, free-text responses and demographic information selected by the Customer. Survey Data may contain Personal Information or Sensitive Information depending on how a survey has been configured.

Platform Data: operational information such as login history, audit logs, system diagnostics, browser and device information, usage statistics, security events and performance metrics. Platform Data helps us maintain security, improve reliability and support customers, and remains the property of Humn.

Benchmark Data: aggregated and appropriately de-identified information derived from multiple organisations, used to develop industry benchmarks, identify emerging workplace trends, improve reporting and the Platform, undertake research and improve analytical models. Benchmark Data is designed so that individuals and participating organisations are not reasonably identifiable, and remains the property of Humn.

Humn Intellectual Property: the software, source code, algorithms, methodologies, scoring and benchmark models, Documentation, reporting frameworks, platform design, trademarks and other intellectual property developed by Humn, which remains the property of Humn unless otherwise agreed in writing.

8. Information we collect

8.1 The information we collect depends on how you interact with the Platform, and may include:

- **Account information:** name, organisation, work email, telephone number, position title, login credentials.
- **Customer information:** organisation details, billing information, subscription information, authorised users, configuration settings.
- **Survey information:** depending on how a survey has been configured, responses relating to psychosocial hazards, work design, leadership, workload, support, change management, workplace relationships, psychological safety, organisational culture, wellbeing indicators, risk maturity, consultation, organisational profile, implementation progress, demographic categories selected by the Customer, and optional free-text responses.

8.2 We encourage customers to minimise the collection of unnecessary personal information within free-text responses wherever reasonably practicable.

9. Sensitive Information

9.1 Some survey responses may constitute Sensitive Information under Australian privacy legislation, for example information relating to mental health, psychological wellbeing, workplace behaviours, bullying, harassment, discrimination, traumatic events or occupational stress.

9.2 Where Sensitive Information is collected, Humn handles it with additional care and applies security controls designed to reduce the risk of unauthorised access or disclosure. Humn collects Sensitive Information only where it is reasonably necessary for the Platform's functions and, where required by law, with the consent of the relevant individual or on another lawful basis. Customers are responsible for providing any collection notices and obtaining any consents required from Respondents.

10. Information we collect automatically

10.1 When you access our website or the Platform, certain technical information may be collected automatically, including IP address, browser type, operating system, device identifiers, pages viewed, session duration, referring website, date and time of access, diagnostic information and error logs. This information assists us to maintain security, improve performance, identify faults, understand usage patterns and protect against unauthorised access.

10.2 **Cookies.** Humn uses cookies and similar technologies to remember preferences, maintain user sessions, understand website usage, improve performance and support security controls. Most browsers allow users to manage or disable cookies through browser settings; disabling cookies may affect some features. Further information is set out in our Cookie Policy.

11. How and when we collect information

11.1 Information may be collected when you visit our website, create an account, purchase our services, complete a survey, participate in workshops or webinars, contact us, subscribe to communications, request support, interact with authorised third-party integrations, or provide information during implementation or consulting engagements. Information may also be provided to us by an organisation administering a survey, or by authorised representatives acting on its behalf.

11.2 **Collection from employers (roles and responsibilities).** In many cases, Humn provides services to organisations that ask their workers to participate in surveys. In these circumstances the organisation (the Customer) determines what information is collected and the purpose of the survey, and Humn provides the technology used to securely host, administer and report on that information and processes it in accordance with the Contract and this Policy. Responsibility for information governance is shared: the Customer determines what information is collected and entered into the Platform, and Humn provides the technology used to host, process, analyse and report on it. Nothing in this Policy transfers responsibility for organisational decision-making or statutory obligations from the Customer to Humn. Where organisations provide collection notices or consent information to Respondents, those notices operate alongside this Policy.

12. Why we collect and how we use personal information

12.1 Humn collects personal information only where it is reasonably necessary to provide our products and services, operate our business, meet our legal obligations, improve the Platform and support our customers. Depending on how you interact with the Platform, we may use personal information to:

- establish and administer customer accounts and authenticate users;
- administer psychosocial risk surveys and related assessments;
- generate reports, dashboards and organisational insights;
- identify trends and emerging workplace risks and facilitate consultation and risk-management activities;

- provide implementation, support and customer success services and respond to enquiries;
- improve the functionality, performance and security of the Platform;
- undertake research and statistical analysis using de-identified information and develop benchmarking datasets;
- comply with applicable laws and regulatory requirements; and
- protect the rights, property and safety of Humn, our customers and users.

12.2 Permitted processing of Customer Data. Humn processes Customer Data only for purposes reasonably necessary to provide the Platform, authenticate users, administer surveys, generate reports and dashboards, support benchmarking, provide technical support and customer success services, undertake implementation services, maintain Platform security and business continuity, improve Platform functionality and comply with legal obligations. Customer Data will not be used for unrelated commercial purposes without the Customer's consent unless required by law.

12.3 How we use survey information. Survey responses are used primarily to assist organisations to understand psychosocial hazards and other workplace factors affecting health, safety and wellbeing, including to calculate psychosocial hazard scores, generate organisational reports, identify patterns across teams or demographic groups, prioritise risks, monitor changes over time, evaluate the effectiveness of risk controls and support consultation. The Platform does not diagnose individuals, assess psychological health or make employment decisions.

12.4 We do not collect personal information unless there is a legitimate business purpose or legal basis for doing so.

13. Ownership of information

13.1 Unless otherwise agreed in writing, Customers retain ownership of Customer Data and Survey Data collected on their behalf, determine how survey projects are configured and administered, and remain responsible for complying with applicable workplace and privacy obligations associated with collecting information from their workers.

13.2 Humn retains ownership of the Platform, software, source code, databases, system architecture, algorithms, scoring and reporting methodologies, benchmark methodologies, Documentation, Platform Data, Benchmark Data and other Intellectual Property developed by Humn. Nothing in this Policy transfers ownership of Humn Intellectual Property to customers.

14. De-identified and aggregated information, benchmarking and research

14.1 Humn may create de-identified and aggregated datasets derived from information processed through the Platform. Before information is included in these datasets, Humn takes reasonable steps to remove or minimise information that could reasonably identify an individual or participating organisation. Aggregated datasets may be used to develop industry benchmarks, improve the Platform and reporting methodologies, validate risk models, understand emerging psychosocial hazards, undertake research and statistical analysis, identify industry trends and improve customer insights.

14.2 Benchmarking is a core feature of the Platform. It enables participating organisations to compare their results with broader industry datasets while preserving confidentiality, using aggregated, de-identified data. Benchmark reports may compare information across industry sectors, organisation size, geographic regions, workforce characteristics, organisational maturity and historical trends. Humn does not sell identifiable customer information or identifiable survey responses and will not identify an individual or participating organisation in published benchmarking information without their prior written consent.

14.3 Research and product development. Where appropriate, de-identified information may be used to improve survey methodology, validate psychosocial measurement models, improve analytics and benchmark quality, identify emerging workplace trends and support academic or industry research. Where research is published externally, no organisation or individual will be identified unless they have expressly agreed to participate.

15. Artificial intelligence

15.1 Humn may use artificial intelligence and machine-learning technologies to improve the Platform and enhance customer insights, for example to identify emerging trends, generate summaries, assist with report preparation, identify recurring themes, improve search functionality and support predictive analytics.

15.2 Where AI is used: human judgement remains essential; AI-generated insights should be reviewed before decisions are made; organisations remain responsible for their own decisions; and AI does not replace legal, psychological or professional advice, and does not independently determine legal compliance, employment outcomes or psychosocial risk controls.

15.3 Where AI models are developed using customer information, Humn will use de-identified and aggregated information wherever reasonably practicable. Humn does not knowingly use identifiable customer information to train publicly available AI models.

16. Disclosure of personal information

16.1 Humn may disclose personal information where reasonably necessary to provide our services or where required by law, including to authorised employees and contractors, cloud hosting and technology service providers, software vendors, professional advisers, auditors, regulators, law enforcement agencies and government authorities where required by law. Recipients are expected to protect information in accordance with applicable legal obligations and contractual requirements.

16.2 Sub-processors and third-party service providers. Humn engages carefully selected service providers to operate the Platform, including providers of cloud infrastructure, authentication, monitoring, communications, payment processing, analytics, customer support and data storage (for example, Amazon Web Services for cloud infrastructure and hosting, and Auth0 for authentication and identity). Where a provider processes personal information on our behalf, Humn takes reasonable steps to ensure it implements appropriate privacy and security controls, assesses and records the provider in a sub-processor register, and remains responsible for ensuring appropriate contractual obligations apply to those providers.

16.3 International processing and data residency. The Platform's production Customer Data is hosted in Australia, in the Amazon Web Services Asia Pacific (Sydney) region, and client support is provided from Australia. Some service providers may store or process limited information outside Australia. Where personal information is transferred internationally, Humn takes reasonable steps to ensure that recipients protect information in a manner consistent with Australian privacy requirements and contractual obligations. The countries in which information is processed may change as our technology providers evolve.

17. Marketing communications

17.1 Humn may send communications relating to product updates, service announcements, webinars, educational resources, events, newsletters and customer insights. Individuals may opt out of marketing communications at any time using the unsubscribe link or by contacting Humn. We will continue to send

essential service-related communications where necessary to administer accounts or provide contracted services.

18. Information security

18.1 Protecting information is fundamental to maintaining trust. Humn implements administrative, technical, physical and organisational safeguards designed to protect Personal Information and Customer Data from unauthorised access, use, disclosure, alteration or loss. These safeguards include:

- encryption of data in transit using TLS 1.2 and 1.3, and encryption of data at rest using AES-256 through a managed key-management service, across the database and its backups, uploaded files, message queues, the cache and secrets;
- secure cloud hosting on Amazon Web Services within a private network, with production Customer Data hosted in the AWS Asia Pacific (Sydney) region, within Australia;
- delegated identity through Auth0, meaning Humn stores no passwords, with single sign-on or passwordless login, role-based access controls, least-privilege access, multi-factor authentication for administrative and remote access, and short-lived, automatically expiring sessions;
- separation of each organisation's data through per-organisation database schema isolation;
- audit logging, security monitoring and alerting;
- vulnerability management, security updates and controlled software releases;
- regular encrypted data backups and tested recovery; and
- staff confidentiality obligations, pre-employment checks and security-awareness training.

18.2 The cloud infrastructure Humn uses (Amazon Web Services) maintains independent third-party attestations for its infrastructure, including SOC 2 and ISO/IEC 27001, with the AWS Sydney region within scope. These attestations cover the underlying infrastructure under the shared responsibility model; Humn remains responsible for the application-level controls it operates.

18.3 Humn's information-security controls, including its hosting architecture, cryptographic standards and security governance, are described in more detail in the Information Security Schedule (Schedule 3). Security controls may evolve to reflect changing technology and emerging cyber-security threats. While Humn takes reasonable steps to protect information, no method of electronic transmission or storage can be guaranteed to be completely secure, and Humn cannot guarantee absolute security.

19. Data retention

19.1 Humn retains information only for as long as reasonably necessary to provide the Platform and associated services, meet contractual obligations, comply with legal and regulatory requirements, resolve disputes, protect our legal interests and improve the Platform using appropriately de-identified information.

19.2 Where information is no longer required, Humn will take reasonable steps to securely delete or de-identify it, unless retention is required or authorised by law. Certain de-identified and aggregated Benchmark Data, and Platform Data, may be retained after Customer Data has been deleted, provided it no longer reasonably identifies any individual or organisation.

20. Return and deletion of Customer Data

20.1 Following termination of the Subscription, Customers may request the export of Customer Data within the period specified in the Platform Subscription Agreement. Following expiry of that period, Humn may securely delete Customer Data unless retention is required by law or under a contractual obligation.

20.2 Deletion of Customer Data does not require deletion of Platform Data, audit logs, security logs, Benchmark Data or information required to be retained by law.

21. Data breach management

21.1 Humn maintains documented incident response and data-breach response plans, including an incident register and a contact tree. Where Humn becomes aware of a confirmed security incident affecting Customer Data or Personal Information, Humn will: promptly investigate the incident; take reasonable steps to contain and remediate it; assess the likely impact; notify the affected Customer without undue delay, and in any event as soon as reasonably practicable after confirming the incident; and cooperate with the Customer in responding to the incident.

21.2 **Notifiable Data Breaches scheme.** Humn and the Customer each acknowledge their respective obligations under the Notifiable Data Breaches scheme in Part IIIC of the *Privacy Act 1988* (Cth). Where an eligible data breach involving Personal Information is likely to have occurred, the Parties will cooperate to assess the breach and, where required, to notify affected individuals and the Office of the Australian Information Commissioner (OAIC) within the timeframes required by law. As between the Parties, the Customer is responsible for notifications relating to information for which it is the controlling entity, unless otherwise agreed in writing. Each Party remains responsible for complying with the legal obligations that apply to it in relation to eligible data breaches.

21.3 This clause is to be read together with the data-breach and incident-response provisions of the Platform Subscription Agreement and the Information Security Schedule (Schedule 3).

22. Audit, assurance and ethical use

22.1 On reasonable written request, Humn may provide information reasonably necessary to demonstrate compliance with its data-processing and security obligations, for example through independent audit reports, security certifications, policy documentation or compliance questionnaires. Direct access to Humn's systems will not ordinarily be provided unless required by law or expressly agreed by the Parties.

22.2 Humn is committed to the ethical use of workplace information. Humn will not knowingly use Customer Data in a manner inconsistent with the purposes for which it was collected, or in a way that would reasonably undermine the trust of customers or Respondents. This commitment applies to Platform development, benchmarking, research and analytical activities.

23. Your rights, access and correction

23.1 Subject to applicable law, individuals may request access to Personal Information held by Humn, request correction of inaccurate or incomplete Personal Information, request that we update contact details, request deletion of information where appropriate, withdraw consent where processing is based on consent, and make a privacy complaint. Requests should be made using the contact details in clause 25. Humn may require reasonable evidence of identity before processing a request.

23.2 Humn will respond within a reasonable period. In some circumstances Humn may be unable to provide access where permitted by law, including where doing so would unreasonably affect the privacy of another individual, prejudice legal proceedings, compromise security or breach contractual obligations. Where access cannot be provided, Humn will explain the reasons unless prohibited by law.

24. Privacy complaints

24.1 If you believe Humn has not handled your Personal Information appropriately, please contact us in the first instance. We will acknowledge your complaint, investigate the matter, respond within a reasonable timeframe and take appropriate action where required. If you are not satisfied with our response, you may lodge a complaint with the Office of the Australian Information Commissioner (OAIC) at www.oaic.gov.au.

25. Contact us

Privacy Officer

Global Psychosocial Safety Network Pty Ltd (ACN 692 420 269 / ABN 17 692 420 269) trading as Humn IQ®

Suite 44, Marnirni-apinhi Building, Lot Fourteen, North Terrace, Adelaide SA 5000

Email: admin@humn.digital

Platform: www.humn.digital

26. Changes to this Privacy Policy

26.1 Humn may update this Privacy Policy from time to time to reflect changes in legislation, technology, business operations, Platform functionality or privacy practices. The most current version will always be published on the Humn website. Where changes are material, we may notify customers through the Platform, by email or by other appropriate means.

Version control

Version	Date	Description
0.1	7 August 2026	Initial draft
1.1	7 August 2026	Information security section expanded with the Platform's actual controls (TLS, AES-256, Auth0, hosting) and named key sub-processors
1.2	7 August 2026	Data residency made specific (AWS Sydney); AWS SOC 2 / ISO 27001 and ISMS framework alignment noted; incident and data-breach response plans referenced