

Foreword

Southern Star Research (the “Company”) collects, holds, uses, discloses and processes personal information (also referred to as data) relating to individuals (also referred to as data subjects), including but not limited to its clients, contractors, suppliers, clinical trial participants and employees. This data is obtained and processed by the Company in order to provide services to our clients and perform our standard business activities. The information collected by the Company will, from time to time, be accessible to certain individuals employed or engaged by the Company who may be required to use the information in the course of their duties.

The Company acts as a data controller by defining how and why personal data is processed in order to perform our duties and provide services to our clients. The Company engages suppliers as processors to process and store information on our behalf and on behalf of our clients.

The Company data controlling and processing activities are regulated by National and International privacy laws, which foster privacy by design. This framework underpins transparent information handling practices and business accountability to give individuals we work with confidence that their privacy is protected. In addition to these privacy laws, our industry is governed by internationally enforceable requirements (ICH Good Clinical Practice and ISO 14155 Clinical investigation of medical devices for human subjects – Good clinical Practice) and the Australian ethical framework (NHMRC National Statement) as well as other international regulations in the countries in which we operate with regard to the use, protection and security of health information obtained from clinical trial participants.

1. Introduction

This Policy sets out the Company’s position in relation to the protection of personal information, as defined under the Privacy Act 1998 (Cth), which includes the Australian Privacy Principles (“APP”) and the European Union General Data Protection Regulation (GDPR) EU2016/679.

This Policy defines how personal information will be controlled and processed in a lawful, fair and transparent manner. The Company will ensure that data is appropriate, accurate and legitimately obtained for business purposes. Information will be kept secure, its integrity maintained and once no longer required, will be destroyed or returned.

HRP 002, v2.0	PRIVACY POLICY	
---------------	----------------	--

The obligations imposed on the Company (a data controller) under this Policy are also imposed on any individual or entity (independent contractors and consultants) engaged by the Company as (“employees”) and (“processors”) who have access to personal information in the course of their duties.

The Company will establish contracts (such as a Data Privacy Addendum) with suppliers providing data processing services, establishing the relationship and terms in accordance with the GDPR.

2. Definitions

"personal information" is information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in material form or not, about an individual whose identity is apparent, or can be reasonably be ascertained, from the information or opinion. This includes a name, an identification number, location data, online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

"sensitive information" is information or an opinion about an individual's: racial or ethnic origin; political opinions; religious beliefs; philosophical beliefs; membership of a professional or trade association; membership of a trade union; sexual preferences; criminal record; health information; genetic information about an individual that is not otherwise health information; or biometric information for the purpose of uniquely identifying a natural person.

A reference to 'personal information' in this Policy includes the meaning of 'sensitive information' unless otherwise indicated.

"unsolicited personal information" is personal information that the Company receives which it did not solicit typically by unauthorized disclosure (for example information sent in a misdirected email).

3. What Is Not Personal Information

The Australian Privacy Principles exclude the collection, holding, use or disclosure of personal information that is an employee record¹.

An employee record is a record of personal information relating to the employment of an employee. Examples of personal employment information include (but are not limited to) health information and information about the

engagement, training, disciplining, resignation, termination, terms and conditions of employment of the employee².

Employees (such as those engaged in a supervisory or human resources capacity) will have access to employee records. Employees who have access to employee records will ensure they are handled confidentially and for proper purposes only. Employee records may only be collected, used and disclosed where the act of doing so is directly related to a current or former employment relationship.

Access and handling of employee records will be supervised and managed by our Human Resources Manager.

- The EU General Data Protection Regulation includes the rights of employees in the EU/EEA (European Union/ Economic Area) to their employment records and therefore records of employment for these employees are not exempt. Specific directives regarding consent requirements for EU employee records are detailed in section 5.*
- Employees located in the EU/EEA may access and correct their employment record on request. The ability to delete EU employee files (the right to be forgotten) is possible where the records are no longer necessary for the purpose they were collected.*

4. Types of Information the Company Collects and Holds

In the course of its usual business practices, Southern Star Research will collect and hold personal information. The Company may also collect sensitive information and in doing so, must have obtained consent in addition to collection being reasonably necessary.

The nature of personal information the Company collects and holds may depend on an individual's relationship with the Company, for example:

Individual Relationship (Data Subject)	Purpose for Information provision	Information Type (Nature)
Candidate	Person seeking employment with the Company.	Name, address, email address, resume, emergency contact, qualifications (including medical registration) and payment details. Additional details may be required for candidates on a working visa.
Employee	Person employed by the Company	Name, address, email address, resume, medical history, emergency contact, taxation details, qualifications (including medical registration), health information and information about the engagement, training, disciplining, resignation, termination, terms and conditions of employment of the employee and payment details. Additional details may be required for candidates on a working visa.
Client	Person or business receiving services from the Company.	Name, address, email address, and contact telephone number, qualifications.

Effective:
01/JUL/2021

CONFIDENTIAL

Page 3 of 11

A Printed or copied QMS document is not a source document. The current document version should be verified at source prior to use.

Supplier	Person or business providing goods or services to the Company.	Name, address, email address, contact telephone number, business records, billing information, professional information including qualification, medical registration, experience, clinical interest and specialities, information about the goods or product.
Referee	Referee of a candidate being considered for employment.	Name, contact details, current employment information and professional opinion of the candidate.
Clinical Trial Participant	Person who is participating in a Clinical Trial conducted by the Company's client.	Subject code/identifier and sensitive information as above

Data protection impact assessments will be conducted as new technologies are implemented and where processing is likely to result in a high risk to rights and freedoms of individuals as defined in Article 35 of GDPR.

5. Consent

The Company will obtain Consent to handle and process personal information. Consent will include details of the purpose for collection and how the data will be processed while in the control of the Company. Where the individual directly supplies personal information to the Company, consent will be inferred.

The Company will ensure that consent is freely given and will provide documentation that is specific, informed and unambiguous. The ability for individuals to withdraw consent at anytime will be clearly documented. Consent will be formalised in contracts, agreements and Participant Information Consent Forms (PICF) depending on the individual, information type and their relationship with the Company¹.

The need for explicit consent to process sensitive information applies to Clinical Trial Participants and this will be clearly defined in the PICF.

¹ Employees located in the EU/EEA have the right to consent to the processing of their employee data however, the company will only collect data it explicitly needs and therefore consent from the employee is not required.

6. How the Company Collects and Holds Personal Information

Southern Star Research (and processors acting on our behalf) collect personal information only by lawful means.

The Company may collect personal information in a number of ways including (without limitation):

- Application forms
- Email or other written mechanisms;
- Over a telephone call

- In person
- Through transactions
- Through the Company website
- Through lawful surveillance means such as a surveillance camera;
- By technology that is used to support communications between individuals and the Company (i.e., instant messaging, voice chat and file sharing platforms);
- Through publicly available information sources (which may include telephone directories, the internet and social media sites); and
- Direct marketing database providers

When the Company collects personal information about an individual through publically available information sources, it will manage such information in accordance with the APPs and EU GDPR.

7. Privacy Notices

At or before the time or, if it is not reasonably practicable, as soon as practicable after, the Company collects personal information, the Company will take steps as are reasonable in the circumstances to either notify the individual or otherwise ensure that the individual is made aware of the following:

- identity and contact details of the Company (Data Controller);
- the Company has collected personal information from someone other than the individual or if the individual is unaware that such information has been collected;
- collection of personal information is required by Australian law, if applicable
- purpose for which the Company collects the personal information;
- consequences if the Company does not collect some/all of the personal information;
- other third party (Data Processor) to which the Company may disclose the personal information;
- length of time the information will be retained;
- if the Company is likely to disclose personal information to overseas recipients, and countries in which those recipients are likely to be located; and
- this privacy Policy and that it contains information about how an individual may exercise their rights regarding their personal information.

8. Use and Disclosure of Personal Information

The purpose for which the Company may use and/or disclose personal information will include (but is not limited to):

- recruitment functions;
- service provision supporting Clinical Trials and associated therapeutic product development activities;
- client service management;
- training and events;
- questionnaires and surveys; and
- business relationship management.

The Company may collect, hold, use and/or disclose personal information if an individual consents or (if required) is authorised under law. Southern Star Research will only provide personal information to third parties, under binding agreements, in accordance with this Policy and as necessary to support the Company in its provision of services.

9. Disclosure of Personal Information

The Company may disclose personal information for any purpose for which it was collected, as indicated under section 4 of this Policy, or where it is under legal duty to do so.

Disclosure may be to internal, related entities or third parties (Data Processors) such as contracted service providers. Disclosure to a third party will be made in accordance with this Policy. Third parties are required (as per binding agreement) to treat information in accordance with the APPs and GDPR as applicable.

Information collected in the EU/EEA may be transferred outside of the region if the EU Commission has approved the receiving country/ies with adequate protection standards. If the country is not approved, the Company will ensure that it has entered into an appropriate agreement (including the data protection clauses) and or binding codes of conduct are in place with the information recipient/processor.

10. Access to Personal Information

If the Company holds personal information about an individual, the individual may request access to that information by putting the request in writing and sending it to the Privacy Officer. The Company will respond to any request within a reasonable period.

The Company may refuse to grant an individual access to personal information in some circumstances for example, requests that will breach Clinical Trial regulations. When applicable, the Company will provide the individual with written notice indicating the reason for the refusal and the mechanisms available to the requestor to make a complaint (as applicable).

All external requests for access to personal information will be directed to the Privacy Officer. Requests from current employees will be directed to the Human Resources Manager with notification to the Privacy Officer.

11. Correction of Personal Information

If the Company holds personal information that is inaccurate, out of date, incomplete, irrelevant or misleading, it will take steps as are reasonable to correct the information.

If the Company holds personal information and an individual makes a request in writing to correct the information, the Company will respond within a reasonable period.

The Company may refuse to collect personal information in some circumstances. When applicable, the Company will give the individual written notice that sets out: the reason for the refusal and the mechanisms available to the individual to make a complaint (as applicable).

If the Company corrects personal information which has been supplied to a third party (Data Processor) and the individual requests the third party is notified of the correction, the Company will take such steps as are reasonable to give that notification unless impracticable or unlawful to do so.

An individual may ask for access or correction of their information by contacting the Privacy Officer by the following means:

Telephone: +61 (0)2 9011 6266
Email: info@SouthernStarResearch.com
By Post: Privacy Officer, Southern Star Research Pty Ltd,
PO Box 52,
Gordon, NSW 2072, Australia

Requests to correct information from employees will be directed to the Human Resources Manager with notification to the Privacy Officer.

12. Integrity and Security of Personal Information

The Company will take steps (if any) as are reasonable in the circumstances to ensure that the personal information that it collects is accurate, up to date and complete.

The Company and our employees take steps as is reasonable in the circumstance to protect personal information from misuse, interference, loss and from unauthorised access, modification or disclosure. This is achieved by holding and storing information in electronic format on a secure server with access restrictions. Hard copy information is retained in locked cabinets with physical access restrictions.


Personal information held by the Company that is no longer required for business purposes or required by law to be retained, the Company will take steps reasonable in the circumstances to destroy or return the information (as applicable). Destruction will take the form of permanent deletion from electronic records including any associated back up. Hard copy information will be shredded or redacted.

13. Anonymity and Pseudonymity

Individuals may remain anonymous, or use a pseudonym, when dealing with the Company in relation to a particular matter. This does not apply:

- where the Company is required or authorised by or under an Australian law, or a court order, to deal with individuals who have identified themselves; or
- where it is impracticable for the Company to deal with individuals who have not identified themselves or who have used a pseudonym.

However, in some cases if an individual does not provide the Company with the personal information when requested, the Company may not be able to respond to the request or provide them with the goods or services that they are requesting.

HRP 002, v2.0	PRIVACY POLICY	
---------------	----------------	--

Pseudonyms (such as participant identification numbers used in clinical trials) will be treated as a form of personal information and treated as such in accordance with this Policy.

14. Additional Rights for Individuals Located in the EU/EEA.

Individuals covered under the jurisdiction of the EU GDPR have the right to data erasure (the right to be forgotten) and may request deletion of their data under certain circumstances, especially where the individual withdraws their consent or the information is no longer required as per section 12 of this Policy.

Clinical Trial Participants may withdraw from clinical trials at any time however, their data will be retained as required by the local competent authority and data collected prior to withdrawal will be controlled and processed as defined in the applicable consent documentation.

Individuals may object at anytime to the processing of their personal data. If an objection is made, processing must stop if allowable (there are defined exceptions to this for the conduct of clinical trials) under local and international laws pertaining to the purpose of collection. All objections for the processing of personal information will be directed to the Privacy Officer. Third parties (Data Processors) receiving processing objections are required to notify the Company in reasonable time in accordance with their data agreements.

15. Complaints

Individuals have a right to complain about the Company's handling of personal information. Complaints should be made in writing and directed to the Privacy Officer. The Company will respond in writing within a reasonable period.

Individuals, who are dissatisfied with the Company's response to a complaint, may refer the complaint to the Office of the Australian Information Commissioner.

16. Privacy Breach

The Company takes its responsibility for the personal information it collects and maintains very seriously. While all duty of care will be exercised the Company may still be involved in privacy breaches. Breaches may occur when personal information is obtained by unauthorised access, disclosure or loss. The company may be involved in breaches originating from or occurring at third parties. When this applies the company will fulfill all applicable breach handling requirements as defined in this section.

When a privacy breach is identified, the Company will take reasonable steps to notify the affected individuals and take measures to mitigate the breach including actions to prevent re-occurrence where possible. All identified breaches will be documented in writing.

When notified of an unauthorised or inadvertent disclosure of personal information, the Company will assess the information to determine if it could have collected the personal information in line with the APP/GDPR. If the Company could not have reasonably obtained the information it will destroy the information. Destruction will take the form of permanent deletion from electronic records including any associated back up. Hard copy information will be shredded or redacted. All identified disclosures will be documented in writing.

All privacy breaches will be assessed within 30 calendar days in order to determine if they require reporting to the local supervisory body. Breaches unlikely to impact the rights and freedoms of individuals will not be reported. Any breach meeting notification criteria will be reported as soon as practical¹. The Company will notify the individual without undue delay should a data breach be deemed likely to result in a high risk to the rights and freedoms of the individual.

If the Company identifies an internal breach i.e. an employee directed by the Company who fails to act in accordance with this Policy will be deemed to have breached this Policy and will be subject to formal counselling and disciplinary action, up to and including possible termination of the employee's employment.

¹ Privacy breaches occurring under the jurisdiction of the GDPR will be reported to the relevant supervisory authority within 72 hours of the Company becoming aware of the breach.

17. Additional Information Regarding Privacy

The Company may update this privacy Policy at any time. The current version in full is available on the Company website in addition to a Policy summary known as the Privacy Statement. Other forms of the Policy are available on request.

Additional information on the Privacy Act and Australian Privacy Principles is available from the Office of the Australian Information Commissioner (www.oaic.gov.au).

18. DOCUMENT REVISION HISTORY

This policy supersedes policy ID: HRP 002, v1.0 Privacy Policy

Changes made

Minor formatting and grammatical amendments for clarification.

Addition of document revision history and authorisation section.

19. DOCUMENT AUTHORISATION

	<i>Name</i>	<i>Position</i>	<i>Signature</i>	<i>Date</i>
Author	David Lloyd	Managing Director	Original Paper Copy Signed	17JUN2021
Reviewer	Tracey Frear	Director, Clinical Operations	Original Paper Copy Signed	24JUN2021
Approver	Kellie Lantry	Quality Assurance Manager	Original Paper Copy Signed	24JUN2021

Policy Template used for this Policy = QA 001-E – Version 1.0, effective 29NOV2018