



ISMS Data Protection Policy

Document Number SKAO-GOV-0000061
Classification: UNRESTRICTED
Document type: POL
Revision 04
Date: 2026-09-09
Status: Released

Role	Name	Designation	Affiliation	Signature	Date
Author	D. McLachrie	Information Security and Data Protection Specialist	SKAO	<i>Deborah McLachrie</i>	14/09/2026
Owner	D. McLachrie	Information Security and Data Protection Specialist	SKAO	<i>Deborah McLachrie</i>	14/09/2026
Approved by / Released by	J. Dempsey	Director-General	SKAO	<i>Jessica T Dempsey</i>	15/09/2026



TABLE OF CONTENTS

1	INTRODUCTION.....	3
2	POLICY STATEMENT	3
3	POLICY SCOPE.....	4
4	PERSONAL DATA PROTECTION PRINCIPLES.....	5
5	PROCESSING SPECIAL CATEGORIES OF PERSONAL DATA.....	11
6	PROCESSING PERSONAL DATA RELATING TO CRIMINAL CONVICTIONS AND OFFENCES	13
7	HANDLING SENSITIVE CULTURAL INFORMATION.....	14
8	ARCHIVING.....	14
9	MARKETING	15
10	RIGHTS OF DATA SUBJECTS.....	16
11	INTERNATIONAL TRANSFER OF PERSONAL DATA	31
12	ACCOUNTABILITY AND GOVERNANCE	34
13	NOTIFICATION OF PERSONAL DATA BREACHES	46
14	NOTIFICATION TO THE SKAO COUNCIL	47
15	NOTIFICATION TO THE DATA SUBJECT	47
16	DEFINITION OF TERMS	48
A	REFERENCES	51
	A.1 Applicable documents	51
	A.2 Reference documents	51
	LIST OF ABBREVIATIONS	52
	DOCUMENT HISTORY	52
	ORGANISATION DETAILS.....	54



1 Introduction

- 1.1 This ISMS Data Protection Policy sets out the framework by which the SKAO safeguards personal data in support of its mission to deliver world-leading radio astronomy facilities. As part of SKAO's Information Security Management System (ISMS), the policy establishes the principles, responsibilities, and controls required to ensure that personal data is processed lawfully, fairly, and transparently, and is protected against unauthorised access, disclosure, alteration, or loss. This ISMS Policy will be reviewed by the Information Security Management Forum (ISMF) annually to ensure accuracy and relevance.

2 Policy Statement

- 2.1 SKAO is an Intergovernmental Organisation (IGO) and as such, has been granted certain privileges and immunities from its Member States. One of the most significant privileges and immunities in this respect is the immunity from jurisdiction, which, first, includes that the organisation is not subject to the jurisdiction of national courts and, second, that the national laws do not directly apply to the SKAO, which, instead, is subject to the rules and regulations it has set up by virtue of its international status. Therefore, although SKAO is not legally bound by data protection legislation within the Member States, SKAO intends to follow the principles of the data protection legislation within the three host countries (Australia, South Africa, and United Kingdom). So far as is practicable, this Policy aligns with the following legislation and favours the legislative aspects that provide the highest protection:

- AUS: [Privacy Act 1988](#)
- AUS: [Privacy and Other Legislation Amendment Act 2024](#)
- RSA: [Protection of Personal Information Act \(POPIA\)](#)
- RSA: [Promotion of Access to Information Act \(PAIA\)](#)
- UK: [UK General Data Protection Regulation \(UK GDPR\)](#)
- UK: [Data Protection Act 2018 \(DPA\)](#)
- UK: [Data \(Use and Access\) Act 2025](#)



- 2.2 Noting SKAO's legal status as an intergovernmental organisation, nothing in this Policy will be deemed or interpreted as a waiver, express or implied, of any privileges or immunities accorded to SKAO by its constituent documents or under international public law.
- 2.3 SKAO holds and processes Personal Data about the SKA Community, Suppliers and other individuals for purposes connected with or arising from its activities, operations, scientific mission, governance. functions, responsibilities and obligations, and for other purposes consistent with its role and objectives.
- 2.4 This Policy describes how SKAO seeks to protect Personal Data and ensure that all SKA Community Members that have access to SKAO information or devices understand the rules governing their use of Personal Data to which they have access in the course of their work. This Policy requires these individuals to ensure that the Data Protection Officer (DPO) is consulted before any significant new data processing activity is initiated to ensure compliance with this Policy.

3 Policy Scope

- 3.1 This Policy forms part of the Information Security Management System (ISMS) for the SKAO. All assets defined within the Information Security Scope document [AD1] are bound by the ISMS.
- 3.2 The Director-General has overall responsibility for ensuring this Policy complies with SKAO's obligations, and that all those under SKAO's control comply with it.
- 3.3 The SKAO DPO has primary and day-to-day responsibility for implementing this Policy, monitoring its use and effectiveness, addressing queries relating to it, and auditing internal control systems and procedures to ensure they are effective.
- 3.4 This Policy applies to all forms of information, including digital and hard copies, which contain personal data. It covers all processing activities, including collection, use, retention, transfer, disclosure, and disposal or personal information.



- 3.5 This Policy applies to individuals in the SKA Community who process Personal Data on behalf of, or under the authority of, SKAO (referred to in this Policy as "SKA Community Members"). Such persons must process personal data only for authorised purposes and ensure that an appropriate processing ground has been identified. These persons must be familiar with this Policy and comply with its terms. They should contact the DPO for further information about this Policy if necessary. Failure to comply may lead to disciplinary action which may result in dismissal. Where the individual is not an employee of SKAO, failure to comply may result in disabled access and/or a contractual review.
- 3.6 The definition of Personal Data can be quite broad across all data protection legislation within the three host countries, and whether certain information is defined as Personal Data or not may depend on the specific circumstances in which the Personal Data will be used. SKAO must ensure all Personal Data it processes is conducted in the best interests of the Data Subject, and appropriate technical and organisational controls are in place to protect the data.
- 3.7 The processing conditions described in this Policy reflect a harmonised SKAO approach aligned to privacy legislation referenced in this Policy. Further information regarding Australian and South African privacy requirements and jurisdiction-specific considerations is provided in the Australian Privacy Applicability Document [TBC – AD2] and South African Privacy Applicability Document [TBC – AD3]
- 3.8 This Policy does not apply where Personal Data has been anonymised to the extent where the Personal Data cannot be used to re-identify a Data Subject.

4 Personal Data Protection Principles

- 4.1 SKAO has aligned its standards for data protection with the principles described in the EU General Data Protection Regulation and included any additional requirements defined within the data protection legislation of the host countries where necessary. These Principles are described in the following sub-sections.

4.2 Lawful

- 4.2.1 Personal data must only be processed where it aligns with one of the below conditions which provides a valid basis under this policy for processing personal data.



- 4.2.2 SKA Community Members must ensure that any Personal Data they are responsible for managing and processing on behalf of, or under the authority of, SKAO has a legitimate reason which has been documented and, where required by policy, reviewed by the DPO. It is their responsibility to ensure they have provided the Data Subject with the purpose of the processing and received their consent, where appropriate. At least one of the above conditions must apply whenever Personal Data is processed by SKA Community Members.
- 4.2.3 When deciding to collect and process Personal Data, SKA Community Members must first consider the following factors:
- What is the purpose for processing the data?
 - Is the processing necessary?
 - Can it reasonably be done in a different way?
 - Is there a choice as to whether to process the data?
 - Who does the processing benefit?
 - After selecting the legitimate reason, is this the same as the legitimate reason the Data Subject would expect?
 - What is the impact of the processing on the Data Subject?
 - Is the individual processing the data in a position of power over the Data Subject whose data is being processed?
 - Is the Data Subject a vulnerable person?
 - Would the Data Subject be likely to object to the processing?
 - Is it possible to stop the processing at any time on request, and has stopping the processing been factored in?
- 4.2.4 **Consent:** Consent must be freely given, specific, informed and unambiguous for the Data Subject's Personal Data to be processed for a specific purpose.
- 4.2.4.1 The request for consent must be clear and require a positive action to opt in (no pre-ticked or opt-out boxes). Consent must be unbundled from other terms and conditions, concise and easy to understand.
- 4.2.4.2 The below details must be recorded for consent, whether written, online or verbal consent is provided:
- SKAOs name and role in relation to the processing
 - Purpose of the processing



- Name of the individual
 - Date
 - Time
 - Context and method of consent
 - Detail of information provided
 - Any third-party controllers who will rely on the consent
 - Whether consent has been withdrawn
- 4.2.4.3 Consent records should be retained in accordance with the Data Retention Schedule.
- 4.2.4.4 Where the Data Subject is under 18, consent shall be obtained from a parent, guardian or other person with appropriate responsibility for the Data Subject. SKAO shall take appropriate steps to verify such consent where necessary. This age requirement does not apply where the Data Subject subscribes to SKAO newsletters, magazines or publications.
- 4.2.4.5 SKAO shall obtain the user's consent before using non-essential cookies or similar technologies on SKAO websites or online applications. Consent shall not be required for cookies or similar technologies that are strictly necessary for the operation, security or functionality of the website or online application.
- 4.2.4.6 The Data Subject shall have the right to withdraw their consent at any time. It must be easy to withdraw consent as it was to provide it.
- 4.2.5 **Contract:** The processing is necessary to fulfil or prepare a contract for the Data Subject.
- 4.2.6 **Legal Obligation:** Processing is necessary to comply with a legal or binding obligation applicable to SKAO.
- 4.2.7 **Vital Interests:** Processing the data is necessary to protect a person's life or in a medical situation.
- 4.2.8 **Public Function:** Processing necessary to carry out a task of public interest or requested by an official authority.



- 4.2.9 **Legitimate Interest:** The processing is necessary for SKAO's legitimate interests. This condition does not apply where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject which requires the protection of Personal Data, especially where the Data Subject is a child or otherwise vulnerable. A formal legitimate interest assessment balancing test is required where the processing presents increased risk, complexity or potential impact on the Data Subject.
- 4.2.10 **Recognised Legitimate Interest:** SKAO may process Personal Data without conducting a balancing test where the processing is necessary for a recognised organisational or public interest purpose that is consistent with this Policy and provides appropriate safeguards for the rights and freedoms of Data Subjects. Such purposes may include safeguarding individuals, responding to emergencies, preventing or detecting unlawful activity, protecting the security of SKAO, supporting public safety, or other purposes recognised under applicable data protection frameworks. In all cases, the processing must be necessary, proportionate, and subject to appropriate technical and organisational safeguards.

4.3 Fair

- 4.3.1 The principle of fairness requires that personal data be processed in a manner that is just and reasonable to the data subject. SKAO must ensure that the data processing activities are not misleading or disproportionately intrusive and that they respect the rights and expectations of the individuals whose data is being processed.

4.4 Transparent

- 4.4.1 SKAO shall process personal data fairly and transparently. We will inform Data Subjects about the collection of their processing, be open and transparent and inform the Data Subject what Personal Data will be collected, the legitimate reasons for processing, and its intended purpose. This shall be communicated to the Data Subject at the point of collection of Personal Data via a privacy notice, where applicable. This applies whether SKAO has collected the data directly from the Data Subject, or from another source.



4.5 Purpose Limitation

- 4.5.1 Personal data must be collected for specified, explicit and legitimate purposes and must not be further processed in a manner incompatible with those purposes. Further processing may be undertaken where it is compatible with the original purpose, including where there is a clear legal, regulatory or public-interest justification. Any further processing must have an appropriate lawful basis and meet all applicable data protection requirements.
- 4.5.2 Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall be considered compatible with the original purposes, provided that appropriate safeguards are implemented to protect the rights and freedoms of Data Subjects. Appropriate safeguards may include, where appropriate, data minimisation, anonymisation or pseudonymisation, technical and organisational measures, access controls, retention controls, and other measures designed to reduce risks to Data Subjects.
- 4.5.3 Where an assessment of further processing is required, the following factors must be considered:
- Any link between the purposes for which the Personal Data was originally collected and the purposes for the further processing
 - The nature of the information concerned (e.g. special categories of Personal Data)
 - The context in which the Personal Data was collected and the relationship between the Data Subject and SKAO
 - The consequences of the intended further processing for the Data Subject
 - The way the information was collected
 - Any contractual rights and obligations with third parties
 - The existence of appropriate safeguards



- 4.5.4 SKA Community Members must only process Personal Data for the purpose for which it was collected or for another purpose where further processing is permitted under applicable SKAO policies. Where a SKA Community Member proposes to process Personal Data for a new purpose, they must ensure that the further processing is permitted under applicable policies and consult the DPO where required before undertaking further processing.

4.6 Data Minimisation

- 4.6.1 SKAO shall only collect Personal Data that is deemed adequate, relevant, and limited to what is necessary to undertake the purpose for which the Personal Data is processed. There must be an explicit legitimate reason for requesting each item of Personal Data.

4.7 Accuracy

- 4.7.1 SKAO shall ensure that Personal Data is accurate and where necessary kept up to date.
- 4.7.2 Data Subjects may request that inaccurate Personal Data relating to them is corrected.
- 4.7.3 SKA Community Members must take all reasonable steps to ensure that Personal Data is kept accurate. The DPO must be informed if Personal Data cannot be kept accurate.

4.8 Storage Limitation

- 4.8.1 SKAO shall not retain Personal Data longer than necessary. The retention period shall depend on the circumstances of each case, the reasons that the Personal Data was obtained, and in a manner consistent with the ISMS Data Protection Policy and ISMS Data Retention Schedule.
- 4.8.2 SKA Community Members must ensure Personal Data is not kept longer than the retention period stated in the Data Retention Schedule, the applicable privacy notices, or as agreed directly with the Data Subject. They must inform the Data Subject and the DPO if Personal Data is still required after the agreed retention period.



4.9 Integrity and Confidentiality (Security)

- 4.9.1 SKAO shall ensure Personal Data is processed in a manner that ensures the appropriate technical and operational security controls are in place to protect the Personal Data from unlawful, unauthorised, or accidental processing, modification, theft, loss, or disclosure.
- 4.9.2 SKA Community Members must consult with the IT Team and DPO to define and implement the appropriate security controls required to protect Personal Data. They must raise a security incident [AD4] immediately where they suspect Personal Data has been compromised or tampered with.

4.10 Accountability

- 4.10.1 SKAO must be able to demonstrate compliance to the above principles.

5 Processing Special Categories of Personal Data

- 5.1 Special Categories of Personal Data, also known as sensitive personal information, requires additional protection because this type of Personal Data could present significant risks to a person's fundamental rights and freedoms if it were to be disclosed. The special categories of Personal Data include information relating to a Data Subject's:

- Racial or Ethnic Origin
- Political Opinions
- Religious or Philosophical Beliefs
- Trade Union Membership
- Genetic Data
- Biometric Data (where used for ID purposes)
- Health
- Sex Life or Sexual Orientation
- Credit Information
- Tax File Number Identification
- Employee Records



- 5.2 This does not include Personal Data relating to criminal allegations, proceedings, or convictions. This type of Personal Data is addressed in the next section of this Policy.
- 5.3 The special categories of Personal Data listed above must only be processed if one of the following conditions are met and an appropriate lawful basis for processing has been identified. This is in addition to compliance requirements documented in section 4 of this Policy:
- 5.3.1 **Explicit consent:** Explicit consent has been received from the Data Subject. Explicit consent must follow the consent requirements, but it must be expressed in words, rather than by any other positive active.
 - 5.3.2 **Employment, Social Security, and Social Protection:** Necessary to fulfil obligations relating to employment, social security, and social protection in law
 - 5.3.3 **Vital Interests:** Is in the vital interests of the Data Subject where the Data Subject is physically or legally incapable of giving consent
 - 5.3.4 **Made Public by the Data Subject:** Processing relates to Personal Data which are made public by the Data Subject
 - 5.3.5 **Legal Claims or Judicial Acts:** Is necessary for processing legal claims or judicial acts
 - 5.3.6 **Substantial Public Interest:** Is necessary for reasons of substantial public interest but provides suitable and specific measures to safeguard the rights and freedoms of the Data Subject (see Appendix A for a list of conditions)
 - 5.3.7 **Health or Social Care:** Is necessary for the purpose of assessing the working capacity of a Data Subject relating to health or social care, ensuring suitable and specific measures are in place to protect the rights and freedoms of the Data Subject



- 5.3.8 **Public Health:** Is necessary for reasons of public interest relating to public health, ensuring suitable and specific measures are in place to protect the rights and freedoms of the Data Subject
- 5.3.9 **Archiving, Research, and Statistics:** Processing is necessary for archiving purposes in the public interest, scientific or historical research, or statistical purposes, ensuring suitable and specific measures are in place to protect the rights and freedoms of the Data Subject
- 5.4 Special Category Personal Data may only be processed by SKAO Personnel, Associates, Affiliate Contractors, third party Data Processors acting on behalf of SKAO and other individuals specifically authorised by SKAO to access or process such data and who are subject to appropriate confidentiality and data protection obligations.
- 5.5 Before processing Special Category Personal Data, the Authorised Person must clearly identify the categories of Personal Data required, the purpose and legal basis for the processing, and any intended disclosures. The individual must notify the DPO where Special Category Personal Data is required and provide the reason for processing it.

6 Processing Personal Data Relating to Criminal Convictions and Offences

- 6.1 SKAO conducts a basic check for criminal convictions as part of the recruitment and employment process. SKAO shall not keep a comprehensive register of criminal offence data and shall not disclose any Personal Data relating to criminal record checks to any one external to the SKAO without explicit written consent from the Data Subject.
- 6.2 SKAO Staff Members must obtain approval from the Director-General prior to requesting a criminal record check on a Data Subject, unless it is conducted as part of the recruitment and employment process. Criminal record checks relating to personnel employed by third-party organisations should be undertaken by the employing organisation in accordance with its own policies and procedures.
- 6.3 Only SKAO Staff with a 'need to know' shall be granted access to any Personal Data relating to criminal convictions. Such information must not be disclosed to any other person, either within or outside SKAO, unless the disclosure is necessary for an authorised organisational purpose, or is otherwise permitted under this Policy. The DPO must be consulted before any intended disclosure outside SKAO, unless immediate disclosure is required to protect an individual or comply with an urgent legal or security requirement.



- 6.4 SKAO shall only process Personal Data relating to criminal convictions and offences where the processing is necessary and proportionate for an authorised purpose and is subject to appropriate safeguards for the rights and freedoms of the Data Subject.
- 6.5 Where applicable, SKAO shall identify and document the relevant lawful basis and additional condition for processing, in accordance with this Policy.

7 Handling Sensitive Cultural Information

- 7.1 SKAO is committed to respecting and protecting sensitive cultural protocols, including the handling of secret or sacred information. We recognise the importance of gaining consent when collecting, storing, or sharing cultural heritage data, ensuring that affected communities retain control over their information. Sensitive cultural information, including traditional knowledge, sacred sites, and communal data, will only be accessed or used with explicit community and individual consent. We will implement strict data security measures to prevent unauthorised access and limit data collection to what is necessary.

8 Archiving of SKAO Records and Information

- 8.1 SKAO will archive certain company information for two distinct purposes. Firstly, documents associated with the formation and history of the SKAO that are an enhancement to our online resources in relation to the publication, "The Square Kilometre Array: A Science Mega-project in the Making, 1990 - 2012" are archived in our History Book Archive. This archiving is crucial for preserving the historical and cultural heritage of the SKAO. Similar works may be produced or published in the future and, where appropriate, may also be subject to archiving arrangements.



- 8.2 Secondly, the SKAO company archive will store all information records highlighted in the Data Retention Schedule.
- 8.3 Both archives are securely maintained and accessible only to authorised personnel. We ensure that all archived data is processed in a manner that respects the rights and freedoms of individuals, maintaining the highest standards of data security and confidentiality. This processing is necessary to document and preserve the history and legacy of the SKAO, as well as to support scientific and historical research endeavours.

9 Marketing

- 9.1 Direct marketing is any communication of advertising, promotional or marketing material directed to individuals, including communications promoting products, services, organisational aims or fundraising activities. This also includes processing activities undertaken to support or enable direct marketing.
- 9.2 In most cases, SKAO will not process Personal Data for direct marketing purposes without obtaining the prior consent of the Data Subject, who will be provided with a link to the SKAO Data Protection Privacy Notice. Each communication will also include a clear mechanism for opting out.
- 9.3 Direct marketing may be sent to corporate email addresses that do not contain personal data such as contact@acme.com. Named addresses (e.g. joe.smith@acme.com) remain subject to this ISMS Data Protection Policy. Communications must be reasonably expected in context and include a clear opt-out mechanism
- 9.4 If SKAO is already in contact with an organisation regarding its activities, then it is possible to “soft opt-in” to send marketing and not gather consent for the communication. However, they still must have a clear opt-out mechanism provided in every communication and be provisioned with access to our SKAO Data Protection Privacy Notice.
- 9.5 There is an additional step to take before making marketing telephone calls to organisations or individuals. Check the relevant countries Do Not Call Registers and adhere to any time restrictions for making these calls.



9.6 SKAO uses personal data to send Data Subjects SKAO newsletters, publications and other communications, such as information about new products, engagement opportunities and outreach activities they have subscribed to. Data Subjects register for the SKAO mailing list and provide their consent to receive this information.

10 Rights of Data Subjects

10.1 Data Subjects have certain rights to their Personal Data which must be respected and complied with. SKAO shall ensure individuals can exercise these rights in a fair and considered manner. These rights are described in the following sub sections.

10.2 Where a Data Subject is not satisfied with the SKAO's response to their request, they have the right to lodge a complaint to the DPO who will escalate their complaint to the appropriate level of authority.

10.2.1 Right to be Informed

10.2.1.1 Data Subjects have the right to be informed about the collection and use of their Personal Data. SKAO shall provide Data Subjects with the following information at the point of data collection where applicable:

- Contact information of the Data Controller
- Contact information of the Data Protection Officer
- What Personal Data will be collected
- The purpose for processing their Personal Data
- The legitimate reasons for the processing
- The category of the Personal Data (only for data not obtained directly from the Data Subject)
- Who the Personal Data will be shared with (e.g. third parties) and which categories of Personal Data
- Detailed information of any transfers to third countries and safeguards in place



- The retention period of the Personal Data or the criteria used to determine the retention period, including details for the data disposal after the retention period
 - The right of access to and the right to rectify their Personal Data
 - The right to object or withdraw consent
 - How to lodge a complaint with the SKAO
 - The recipient or categories of recipients of the Personal Data, if any
 - The source of the Personal Data, and whether it came from publicly available sources (only for data not obtained directly from the Data Subject)
 - The details of the existence of automated decision making, including profiling and information about how those decisions are made, their significances and consequences to the Data Subject
- Whether the provision of Personal Data is part of a statutory or contractual requirement or obligation and possible consequences for any failure to provide the data (only for Personal Data obtained directly from the Data Subject)
- 10.2.1.2 SKAO shall provide a privacy notice, available at the point of data collection, that provides the appropriate information stated above where it collects Personal Data from a significant number of Data Subjects. Privacy notices shall be concise, transparent, intelligible, easily accessible, use clear and plain language, and be provided free of charge.
- 10.2.1.3 Staff Resources must ensure the privacy notice is kept accurate. They must inform the DPO if the privacy notice needs to be updated. Privacy notices containing inaccurate information must be updated and republished as soon as practicable. The DPO shall conduct a review of all SKAO privacy notices on an annual basis.



- 10.2.1.4 Staff Resources must provide the relevant information listed above at the point of collection to individual Data Subjects or small groups of Data Subjects using the written communication method used to request the Personal Data. They must retain this communication information and inform the DPO of the Personal Data request.
- 10.2.1.5 Staff Resources must inform the Data Subject, and obtain consent where applicable, if Personal Data needs to be used for a new purpose or disclosed to a third party. Where a privacy notice exists, this must be updated to include the details of the new purpose or third party and published prior to using the Personal Data for the new purpose or disclosing it to a third party.
- 10.2.1.6 Where SKAO receives Personal Data of Data Subjects from other sources, SKAO shall inform the Data Subject that they have received their Personal Data within one month, unless the Data Subject already has the information, providing the information is impossible or would involve disproportionate effort, obtaining or disclosing the Personal Data is required by law, the Personal Data must remain confidential under an obligation of professional secrecy, or providing the information would render impossible or seriously impair the achievement of the objectives of the processing. . SKAO shall also provide the Data Subject with details of the source of the information, plus the relevant information listed in the bullet points above.

10.2.2 Right of Access

- 10.2.2.1 Data Subjects have the right to access and receive a copy of their Personal Data including any other supplementary information, and ensure their Personal Data is being processed fairly. SKAO shall provide Data Subjects, or a third party on their behalf, with a means of requesting this access or a copy of their Personal Data via a Subject Access Request free of charge. SKAO shall respond to such requests within one month of receipt of the request but reserves the right to increase this by a further two months if the request is complex or multiple requests are received from, or regarding, the same Data Subject.



- 10.2.2.2 Subject Access Requests can be made verbally or in writing, including on social media. However, SKAO would like to request that all queries concerning data protection should, if possible, be sent to the SKAOs Data Protection Officer using the contact details provided below. All queries will be recorded and addressed appropriately.
- 10.2.2.3 Where a Subject Access Request is raised on behalf of a Data Subject, the third party must provide sufficient evidence of their authority to raise the request and the authority to access or obtain the Data Subjects Personal Data.
- 10.2.2.4 Where a Subject Access Request is raised by a child, SKAO shall respond directly to the child if it believes the child understands their rights. Otherwise, it reserves the right to respond to the child's parent or guardian.
- 10.2.2.5 SKAO reserves the right to refuse to comply with a Subject Access Request if it would also identify another Data Subject, or for reasons described in the Restrictions Relating to Data Subjects Rights section of this Policy. All reasonable steps to comply with the request, including the redaction of details about another Data Subject, shall be taken before refusing a request. If a request for access is refused, SKAO shall provide the Data Subject with the reason.
- 10.2.2.6 The following examples of exemptions reflect recognised data protection principles adopted by SKAO for the purposes of this Policy and in alignment with the UK GDPR. Any restriction or refusal shall be assessed on a case-by-case basis and applied only where necessary and proportionate.
- Crime and taxation: general
 - Crime and taxation: risk assessment
 - Legal professional privilege
 - Functions designed to protect the public
 - Regulatory functions relating to legal services, the health service and children's services



- Other regulatory functions
- Judicial appointments, independence, and proceedings
- Journalism, academia, art and literature
- Research and statistics.
- Archiving in the public interest
- Health, education and social work data
- Child abuse data
- Management information
- Negotiations with the requester
- Confidential references
- Exam scripts and exam marks
- Where it would pose a serious threat to the life, health, or safety of any individual
- It would impact on the privacy of others
- Where providing the information would be unlawful
- Include information in connection with a commercially sensitive decision-making process.
- Other exemptions

10.2.2.7 Subject Access Requests received by SKAO Staff Resources must be forwarded immediately to the DPO, by email (dpo@skao.int), for consideration and action in accordance with this Policy.

10.2.2.8 SKAO will respond to Data Subject rights requests without undue delay and normally within one month. SKAO may extend this period where a request is complex or multiple requests have been received, request clarification where necessary, limit searches to those that are reasonable and proportionate, or refuse requests that are manifestly unfounded or excessive.



10.2.2.9 Once a Subject Access Request has been made, SKAO Staff Resources must not add, modify, or remove any of the Personal Data relating to the Data Subject that has been requested.

10.2.2.10 SKAO shall conduct a reasonable search for the Personal Data and shall either provide direct access to this information or provide this information in an accessible, concise, intelligible, and commonly used format, which shall be disclosed securely to the Data Subject, or authorised third party, free of charge.

10.2.2.11 SKAO shall not disclose any Personal Data requested as part of a Subject Access Request until it is satisfied that the identity of the Data Subject, or authorised third party, is confirmed.

10.2.3 **Right to Rectification**

10.2.3.1 Data Subjects have the right to have inaccurate Personal Data rectified or completed if it is incomplete. Data Subjects also have the right to restrict processing until the Personal Data has been rectified.

10.2.3.2 SKAO shall rectify or amend the Personal Data of the Data Subject where it is satisfied that it is inaccurate or incomplete. This shall be completed without delay, and within one month. SKAO reserves the right to increase this by a further two months if the request is complex or multiple requests are received from the same Data Subject.

10.2.3.3 SKAO shall contact other organisations that process the Data Subjects Personal Data on its behalf and inform them of the Data Subjects rectification request. SKAO shall communicate this activity to the Data Subject.



- 10.2.3.4 SKAO shall only process such requests if the identity of the Data Subject is confirmed.
- 10.2.3.5 SKAO shall inform the Data Subject if the changed information has an impact on decisions that have been made or will be taken because of the change.
- 10.2.3.6 SKAO reserves the right to refuse to comply with a rectification request for reasons described in the Restrictions Relating to Data Subjects Rights section of this Policy. If a request for rectification is refused, SKAO shall provide the Data Subject with the reason.
- 10.2.3.7 Staff Resources must inform the DPO if they are unable to complete a rectification request due to a particular issue or within the stipulated timeframe.

10.2.4 **Right to Erasure**

- 10.2.4.1 Data Subjects have the right to have their Personal Data erased under certain circumstances, outlined below. This is also known as the 'right to be forgotten'. Such requests shall be completed without delay, and within one month. SKAO reserves the right to increase this by a further two months if the request is complex or multiple requests are received from the same Data Subject.
- 10.2.4.2 SKAO shall erase the Personal Data of a Data Subject where one of the following conditions applies:
 - The Personal Data is no longer necessary for the purpose for which it was originally collected or processed
 - The Data Subject withdraws their consent on which the processing is based, and there is no legal or legitimate ground for processing
 - The Data Subject objects to processing and there is no overriding legitimate interest to continue the processing
 - The Personal Data is being processed for direct marketing purposes, and the Data Subject objects to that processing
 - The Personal Data was unlawfully processed or otherwise breached data protection legislation
 - Erasure must take place to comply with a legal obligation



- The processing relates to a child
- 10.2.4.3 SKAO shall communicate the request for erasure of Personal Data to the relevant third parties unless this proves impossible or involves disproportionate effort. SKAO shall inform the Data Subject of those third parties, if requested.
- 10.2.4.4 Where Personal Data has been made public in an online environment (e.g. social networks or websites) the SKAO shall take reasonable steps to inform other Data Controllers who are processing the Personal Data to erase links to, copies or replication of that Personal Data. The exception to this is where the removal of their Personal Data impacts other Data Subjects or would otherwise be difficult to remove. In which case, the removal of Personal Data will only occur where the majority of Data Subjects request its removal, or to protect the legitimate interests of the Data Subject.
- 10.2.4.5 As part of the erasure request, SKAO shall endeavour to erase the Personal Data of Data Subjects contained within backups where technical mechanisms allow. Where this is not possible, backup media will either be overwritten over time or wiped or disposed in a secure manner when no longer required.
- 10.2.4.6 SKAO shall only process such requests if the identity of the Data Subject is confirmed.
- 10.2.4.7 SKAO reserves the right to refuse to comply with a right to erasure request under the following circumstances:
- To exercise the right of freedom of expression and information (this includes journalism and academic, artistic and literary purposes)
 - For reasons described in the Restrictions Relating to Data Subjects Rights section of this Policy
- 10.2.4.8 If a request for erasure is refused, SKAO shall provide the Data Subject with the reason.
- 10.2.4.9 All requests received by Staff Resources relating to the right to erasure must be forwarded immediately to the DPO for consideration and action in accordance with this Policy.



10.2.5 Right to Restrict Processing

10.2.5.1 Data Subjects have the right to request the restriction or suppression of processing their Personal Data under certain circumstances. Such requests shall be completed without delay, and within one month. SKAO reserves the right to increase this by a further two months if the request is complex or multiple requests are received from the same Data Subject.

10.2.5.2 SKAO shall restrict or suppress the processing of Personal Data of a Data Subject where one of the following conditions applies:

- The accuracy of the Personal Data is contested by the Data Subject, for a period to allow SKAO to verify the accuracy of the Personal Data
- The processing is unlawful and the Data Subject opposes the erasure of the Personal Data and requests the restriction of its use instead
- SKAO no longer requires the Personal Data for the purpose of the processing, but the Data Subject requires the Personal Data to be kept for the exercise or defence of legal claims
- The Data Subject has objected to processing, SKAO is considering their objection request and verifying whether the legitimate interests of SKAO override those of the Data Subject

10.2.5.3 SKAO shall communicate the request for restriction of processing to the relevant third parties unless this proves impossible or involves disproportionate effort. SKAO shall inform the Data Subject of those recipients, if requested.

10.2.5.4 SKAO shall not process restricted Personal Data in any way except to store it, unless:

1. SKAO has the *Data Subjects* consent
2. For reasons described in the Restrictions Relating to *Data Subjects* Rights section of this Policy



- 10.2.5.5 SKAO shall inform the Data Subject in advance of lifting any restrictions and continuing with processing.
- 10.2.5.6 SKAO shall only process such requests if the identity of the Data Subject is confirmed.
- 10.2.5.7 All requests received by SKAO Staff Resources relating to the right to restrict processing must be forwarded immediately to the DPO for consideration and action in accordance with this Policy.

10.2.6 Right to Data Portability

- 10.2.6.1 Data Subjects have the right to data portability of their Personal Data processed electronically. Such requests shall be completed without delay, and within one month. SKAO reserves the right to increase this by a further two months if the request is complex or multiple requests are received from the same Data Subject.
- 10.2.6.2 SKAO shall provide the Data Subject with their Personal Data in a structured, commonly used, machine-readable format (e.g. .CSV, .XML) transmitted in a secure manner, to allow them to reuse it for their own purposes, or SKAO shall send it directly to another Data Controller where technically feasible, if requested by the Data Subject. SKAO shall verify the accuracy of the Personal Data with the Data Subject prior to transferring it to another Data Controller. SKAO shall only process data portability requests if the identity of the Data Subject is confirmed.
- 10.2.6.3 SKAO reserves the right to refuse to comply with a request to data portability where:
 - SKAO has created additional data based on the *Personal Data* provided by the *Data Subject* (only *Personal Data* will be provided)
 - The *Personal Data* has been anonymised
 - The *Personal Data* includes information about other *Data Subjects* who have not provided consent
 - The *Personal Data* was not processed digitally
 - The transfer to another *Data Controller* is not technically feasible
 - The export of *Personal Data* is not technically feasible
 - For reasons described in the Restrictions Relating to *Data Subjects Rights* section of this Policy



- 10.2.6.4 If a request for data portability is refused, SKAO shall provide the Data Subject with the reason.
- 10.2.6.5 Where SKAO is the recipient Data Controller of a data portability request, it shall follow the seven principles relating to the processing of Personal Data stated in this Policy.
- 10.2.6.6 All requests received by Staff resources relating to data portability must be forwarded immediately to the DPO for consideration and action in accordance with this Policy.

10.2.7 **Right to Object**

- 10.2.7.1 Data Subjects have the right to object to the processing of their Personal Data under certain circumstances. The objection may be in relation to all Personal Data, specific Personal Data, or the purpose for processing. Such requests shall be completed without delay, and within one month. SKAO reserves the right to increase this by a further two months if the request is complex or multiple requests are received from the same Data Subject.
- 10.2.7.2 SKAO shall inform the Data Subject of their right to object at the first point of communication, (e.g. in a privacy notice) and state the process for which the objection should be raised.
- 10.2.7.3 Data Subjects have the absolute right to object to the processing of their Personal Data used for the purpose of direct marketing at any time and includes any profiling of Personal Data relating to direct marketing. SKAO shall ensure the Data Subject is provided with a means to object, which should be automated where possible. The SKAO reserves the right to retain just enough Personal Data of a Data Subject to ensure that their preference to direct marketing is respected in future.
- 10.2.7.4 Data Subjects must provide a specific reason to object to the processing of their Personal Data (excludes direct marketing).



10.2.7.5 Data Subjects have the right to object to the processing of their Personal Data for the following purposes based on the personal circumstances of the Data Subject:

- For the performance of a task carried out in the public interest
- For the exercise of official authority vested in SKAO
- SKAO legitimate interests (or those of a third party)

10.2.7.6 However, SKAO reserves the right to refuse to comply with a request objecting to the processing of Personal Data where:

- SKAO is unable to confirm the identity of the Data Subject
- SKAO has legitimate grounds for processing which override the interests, rights and freedoms of the Data Subject
- For reasons described in the Restrictions Relating to Data Subjects Rights section of this Policy that do not conflict with the rights of the Data Subject listed above

10.2.7.7 SKAO shall consider the circumstances of the request and make its decision based on the Data Subjects interests, rights, and freedoms, and the SKAO's legitimate interests. If a request objecting to the processing of Personal Data is refused, SKAO shall provide the Data Subject with the reason.

10.2.7.8 All requests received by Staff Resources relating to objections to processing must be forwarded immediately to the DPO for consideration and action in accordance with this Policy. This excludes requests to object to direct marketing which must be respected and addressed promptly.



10.2.8 Rights in Relation to Automated Decision Making, Including Profiling

10.2.8.1 Automated individual decision-making is a decision made based solely on automated processing, where there is no meaningful human involvement in the taking of the decision. A significant decision is a decision which produces a legal effect for the Data Subject or has a similarly significant effect on the Data Subject. If there is human involvement, such involvement must be meaningful and not merely a token review of an automated recommendation. The person reviewing the decision must have sufficient authority and competence to consider the relevant information and, where appropriate, change or overturn the automated outcome.

10.2.8.2 SKAO shall respect the rights of Data Subjects in relation to automated decision-making and profiling in accordance with applicable data protection legislation.

10.2.8.3 Where SKAO takes a significant decision based solely on automated processing, it shall implement the appropriate safeguards. These safeguards shall include:

- providing the Data Subject with information about the significant decision;
- providing the Data Subject with an opportunity to make representations about the decision;
- providing the Data Subject with the right to require human intervention in the decision; and
- providing the Data Subject with the right to contest the decision.

10.2.8.4 SKAO shall not take a significant decision based solely on automated processing where the decision is based entirely or partly on the processing of special category Personal Data unless the conditions permitted by applicable data protection legislation are met. These include where:

- the Data Subject has given explicit consent to the processing on which the decision is based; or
- the decision is necessary to enter into or perform a contract with the Data Subject, or is required or



authorised by law, and the use of the special category Personal Data is necessary for a substantial public interest and appropriate safeguards are in place to protect the Data Subject's rights and freedoms.

- Where automated decision-making is conducted, SKAO shall:
 - assess and document the risks associated with the processing and, where required, complete a Data Protection Impact Assessment (DPIA);
 - implement appropriate technical and organisational measures to protect the rights, freedoms and legitimate interests of Data Subjects;
 - provide Data Subjects with clear and accessible information about significant decisions taken solely through automated processing, including information required by applicable transparency obligations;
 - ensure that any human intervention is meaningful and capable of influencing or reconsidering the decision; and
 - undertake appropriate testing, monitoring and review to ensure that automated processing operates as intended and remains compliant with applicable data protection legislation.

10.2.9 Restrictions Relating to Data Subject Rights

10.2.9.1 SKAO may restrict or refuse comply with any of the rights stated within this Policy for any of the reasons stated below:

- Where the life or physical safety of the Data Subject would be endangered
- To safeguard national security, defence, or public security
- Where it infringes SKAOs Privileges or Immunities
- Where the information contains financial, commercial, scientific, or technical information, which could cause harm to SKAO if disclosed
- For the protection of the rights and freedoms of the Data Subject and others, including those related to trade secrets



- To safeguard against abuse or unlawful access or transfer
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority
- Where the Personal Data is to be used for the establishment, exercise, or defence of legal claims
- For public health purposes in the public interest
- For archiving purposes in the public interest, scientific or historical research, or statistical purposes
- The request is manifestly unfounded or excessive or vexatious in nature

10.2.9.2 Any restriction or refusal shall be applied only where permitted by this ISMS Data Protection Policy and to the extent necessary and proportionate in the circumstances.

10.2.10 **Right to Lodge a Complaint to SKAO**

10.2.10.1 As SKAO is an Intergovernmental Organisation, the established Supervisory Authorities, or equivalent, in the respective Member States have no jurisdiction over SKAO. SKAO has established its own complaints procedure [TBD.002] to allow Data Subjects to make a formal complaint if they feel their Personal Data or rights have not been used or addressed in keeping with the terms of this Policy . SKAO requests that all complaints are submitted in writing using the contact details below.

Title	Data Protection Officer
Address	SKA Observatory, Jodrell Bank, Lower Withington, Macclesfield, Cheshire, SKA11 9FT, United Kingdom
Email	dpo@skao.int



10.2.10.2 Where the Data Subject is not satisfied with the response from SKAO, they have the right to appeal. The appeals process is described in [TBD.003].

11 International Transfer of Personal Data

11.1 If it is necessary for SKAO to transfer Personal Data outside the relevant SKAO host country, SKAO shall follow the transfer requirements set out in this Policy to protect the rights and fundamental freedoms of Data Subjects and ensure that the level of protection provided to the Personal Data is not materially lower than the level of protection provided in the relevant host country.

11.2 Transfer Restrictions

11.2.1 Transfers Not Requiring Additional Safeguards

11.2.1.1 No additional transfer safeguards shall be required where:

- SKAO transfers Personal Data to a host country where the Personal Data is still collected, managed, and processed by SKAO in accordance with this Policy;
- SKAO only transfers Personal Data directly to each Data Subject, or receives Personal Data directly from each Data Subject;
- Personal Data is transferred to a recipient in the European Economic Area (EEA); or
- Personal Data is transferred to a recipient in a country or territory recognised as providing an adequate level of data protection in alignment with applicable data protection legislation.



11.2.2 Transfers Requiring Safeguards

11.2.2.1 Where a transfer is not covered by an adequacy decision or the UK – US Data Bridge, SKAO shall, where it is able to do so in accordance with its status as an Intergovernmental Organisation, ensure that an appropriate transfer safeguard or other lawful transfer mechanism is in place. Where no such safeguard or mechanism can be put in place, the transfer may only take place where a specific derogation applies, as set out in Section 11.3.

11.2.3 Assessment of Transfers

11.2.3.1 Where required, SKAO shall undertake and document an appropriate assessment of the transfer to ensure that the level of protection provided to the Personal Data is not materially lower than the host country protection.

11.2.4 Third Party Processing

11.2.4.1 Where SKAO shares Personal Data with a third party, a written contract or other legally binding agreement must be in place before the Personal Data is shared, unless a specific derogation applies as set out in Section 11.3. The agreement shall set out the appropriate data protection, confidentiality and security requirements and shall reflect the respective roles and responsibilities of the parties.

11.2.4.2 Where the third-party acts as a processor on behalf of SKAO, the agreement shall include the required processor obligations. Where the parties act as joint controllers, the agreement shall set out their respective responsibilities for the processing. Where the third-party acts as an independent controller, the agreement shall set out the terms governing the sharing and subsequent processing of the Personal Data.



11.2.5 Processing Within SKAO Member States

11.2.5.1 Personal Data processed by third parties within a SKAO Member State is protected by SKAO's privileges and immunities. Any transfer of Personal Data outside the SKAO Member States shall be subject to appropriate prior review and approval in accordance with SKAO's internal governance arrangements.

11.2.6 UK – US Data Bridge

11.2.6.1 Personal Data may be transferred to an organisation in the United States where that organisation is certified under, and participates in, the UK-US Data Bridge, or any successor or replacement framework with prior review and approval in accordance with SKAO's internal governance arrangements.

11.2.7 Purpose Limitation

11.2.7.1 Personal Data transferred under this section shall only be processed for the purposes for which it was transferred and in accordance with this Policy and applicable data protection requirements.

11.3 Derogations for Specific Situations

11.3.1 Where an appropriate transfer safeguard cannot be put in place, a transfer of Personal Data to an organisation or entity in another country may only take place where a specific derogation applies. The transfer must be necessary and proportionate in the circumstances, and the derogation must be assessed and documented on a case-by-case basis.

11.3.2 Such derogations may include where:

- the Data Subject has explicitly consented to the transfer;
- the transfer is necessary for the performance of a contract between the Data Subject and SKAO, or for the implementation of pre-contractual measures taken at the Data Subject's request;
- the transfer is necessary for important reasons of public interest;
- the transfer is necessary for the establishment, exercise or defence of legal claims; or



- the transfer is necessary to protect the vital interests of the Data Subject or another individual where the Data Subject is physically or legally incapable of giving consent.
- 11.3.3 Any transfer relying on a derogation shall be assessed and approved by the Legal Team before the transfer takes place and shall be documented in accordance with SKAO's applicable procedures.

12 Accountability and Governance

12.1 SKAO primarily determines the purposes and means of processing Personal Data and therefore primarily acts as a Data Controller. Where SKAO engages third parties to process Personal Data on its behalf, those parties shall act as Data Processors under written agreements that define the parties' respective responsibilities.

12.1.1 Responsibilities of the Data Controller

- 12.1.1.1 SKAO values the trust provided by Data Subjects and takes its responsibilities to fairly and securely collect, process, and store their Personal Data seriously. SKAO shall conduct the following activities to monitor its overall data protection posture with data protection legislation, identify areas for improvement, and demonstrate its compliance with this Policy:
- Be open and transparent with Data Subjects when collecting, processing, and storing their Personal Data (e.g. implementing privacy notices)
 - Taking a 'data protection by design' approach
 - Implementing appropriate security controls
 - Conducting risk assessments to ensure the appropriate security controls are in place
 - Conducting data protection impact assessments for uses of Personal Data that are likely to result in a high risk to Data Subjects interests
 - Conducting internal departmental audits to ensure compliance with this Policy and associated procedures
 - Conducting technical audits to ensure the effectiveness of the security controls in place



- Maintaining records relating to consent, Data Subject requests, processing activities, results of audits, and evidence of compliance with this Policy
- Ensuring the appropriate data protection requirements and responsibilities are included within contracts with organisations that process Personal Data on behalf of SKAO
- Recording and reporting Personal Data breaches in a timely manner
- Appointing a Data Protection Officer
- Provide training and guidance to Staff Resources
- Monitoring changes to data protection legislation
- Reviewing this Policy and all privacy notices annually and, where required, updating them to reflect significant changes.
- SKAO shall establish a Records of Processing Operations relating to the Personal Data it processes

12.1.2 Security of Processing

12.1.2.1 This Data Protection Policy forms part of SKAO's Information Security Management System (ISMS) which is based on ISO 27001:2022 [RD1] and shall be read in conjunction with relevant ISMS policies, standards and procedures. In particular, the protection of Personal Data shall be supported by SKAO's Incident Response Procedure [AD4], Information Security Policy [AD5], Information Classification, Labelling and Handling Policy [AD6], Access Control and Physical Security Policy [AD7], Data Retention Policy [AD8] and Data Retention Schedule [AD9], Information Security in Supplier Relationships Policy [AD10] Risk Assessment Methodology [AD11], Network and Operational Security Policy [AD12], Artificial Intelligence Policy [AD13], Security Requirements of Information Systems [AD14], Acceptable Use Policy [AD15] and SKA Community Acceptable Use Policy [TBD – AD16]. These documents establish complementary organisational and technical controls for protecting Personal Data throughout its lifecycle.



12.1.2.2 The SKAO ISMS includes, but is not limited to, the following information security practices that have been designed to protect information, including Personal Data:

- Conducting risk assessments based on confidentiality, integrity, and availability to ensure the appropriate level of security is in place [AD12]
- Conducting technical and organisational audits to ensure compliance with the ISMS and assessing the effectiveness of the security controls in place
- Conducting annual reviews of all ISMS policies and associated procedures
- Implementing security zones and network segmentation [AD13]
- Implementing vulnerability management procedures
- Defining requirements for cryptography (encryption)
- Implementing logging, monitoring, and alerting mechanisms
- Implementing the appropriate physical security controls [AD7]
- Classifying, labelling, and handling information [AD6]
- Defining data retention guidelines [AD8] [AD9]
- Implementing security requirements for information systems [AD15]
- Implementing security controls on mobile devices, such as mobile phones and laptops
- Implementing incident management and reporting procedures [AD10]
- Ensuring the appropriate backups and redundancy is in place to allow SKAO to restore information in the event of an incident
- Implementing the secure disposal or re-use of equipment, and decommissioning of cloud-hosted services and environments
- Providing regular information security awareness training to all Staff Resources



12.1.2.3 In addition to the security practices listed above, the following security requirements are mandatory during the collection, processing, and storing of Personal Data:

- Personal Data must be encrypted in transit and at rest
- Access to Personal Data must require authentication and be restricted to SKAO Community members who require access as part of their role, and Data Subjects who require access to their own Personal Data (where applicable)
- Multi-factor authentication must be used where reasonably practicable when accessing information systems containing Personal Data.
- Personal Data must only be retained in alignment with the Data Retention Schedule. [AD9]
- Email systems, information systems, and file systems that either contain or have the potential to contain Personal Data must not be accessed by or stored on non SKAO devices
- Personal Data must not be stored on removable media unless the document, dataset, or information asset containing the Personal Data has been classified as Unrestricted Data in accordance with the Information Classification Policy.
- Personal Data recorded in paper form must be securely locked away when not in use and must not be accessible to unauthorised individuals
- Personal Data recorded in paper form must be disposed of in confidential waste bins when no longer required

12.1.2.4 Also consider the use of anonymisation or pseudonymisation techniques to reduce the risk to Data Subjects whilst allowing SKAO to meet its requirements. Anonymisation places the Personal Data out of scope for data protection regulations, but extreme care must be taken to ensure the anonymised data cannot be traced back to or identify a Data Subject based on the information that is provided. Pseudonymisation is still in scope for data protection legislation, as the Personal Data can be traced back to a Data Subject via a unique identifier.



- 12.1.2.5 SKA Community Members are responsible for creating, collecting, accessing, processing, managing, or maintaining Personal Data under the authority of SKAO must consult with the IT Team and DPO to define and implement the appropriate security controls required to protect Personal Data. This requirement applies to the implementation of new IT Systems and to changes or modifications to existing IT Systems containing Personal Data.
- 12.1.2.6 SKA Community Members must inform the IT Team and the DPO (dpo@skao.int) if they identify a potential breach or potential risk to the security of Personal Data. All reported potential breaches and risks must be managed in accordance with SKAO's incident management procedures.

12.1.3 Data Protection Impact Assessment

- 12.1.3.1 Data Protection Impact Assessments (DPIAs) provide a means for SKAO to assess processing activities and identify, assess and minimise data protection risks.
- 12.1.3.2 SKAO shall complete a DPIA before commencing processing where the processing is likely to result in a high risk to the rights and freedoms of Data Subjects.
- 12.1.3.3 A DPIA must be conducted where processing is likely to result in a high risk to the rights and freedoms of Data Subjects. This includes, but is not limited to, processing where SKAO:
- Uses systematic and extensive profiling or automated decision-making that produces legal effects or similarly significantly affects Data Subjects;
 - Processes Personal Data that could endanger the physical health or safety of Data Subjects in the event of a security breach;
 - Processes Special Category Data or Personal Data relating to criminal convictions and offences on a large scale;
 - Systematically monitors a publicly accessible area on a large scale;
 - Conducts profiling on a large scale;



- Processes biometric data for the purpose of uniquely identifying Data Subjects;
- Processes genetic data;
- Combines, compares or matches Personal Data from multiple sources;
- Processes Personal Data involving the tracking of Data Subjects' online or offline behaviour;
- Uses innovative technologies or applies existing technologies in a novel way;
- Processes Personal Data relating to children or other vulnerable individuals where the processing is likely to result in a high risk to their rights and freedoms; or
- Undertakes other processing which, considering its nature, scope, context and purposes, is likely to result in a high risk to the rights and freedoms of Data Subjects.

12.1.3.4 DPIAs must include, at a minimum:

- A description of the nature, scope, context and purposes of the processing;
- An assessment of the necessity and proportionality of the processing, including the applicable lawful basis and compliance with the data protection principles;
- An assessment of the risks to the rights and freedoms of Data Subjects, including the likelihood and severity of those risks; and
- The measures proposed to address, eliminate or mitigate those risks and demonstrate compliance with applicable data protection requirements.
- The DPIA must record the DPO's advice and recommendations, the outcome of the assessment, any required actions and the residual risks associated with the processing.

12.1.3.5 DPIAs shall be conducted and documented by the DPO, in consultation with the SKA Community Members where required.



- 12.1.3.6 SKA Community Members must provide the DPO with the information necessary to conduct the DPIA and must cooperate with the DPIA process where required.
- 12.1.3.7 The DPO shall assess the identified risks, provide advice on appropriate measures to mitigate those risks, and make recommendations regarding the proposed processing.
- 12.1.3.8 Where a DPIA identifies residual risks that remain high and cannot be sufficiently mitigated, the DPO shall escalate the matter in accordance with SKAO's data protection and information security risk management procedures.
- 12.1.3.9 DPIAs must be reviewed periodically and whenever there is a significant change to the nature, scope, context or purpose of the processing, or where there is reason to believe that the processing may no longer be adequately addressed by the DPIA.
- 12.1.3.10 Audits must be conducted annually for processing activities where a DPIA has been completed.

12.1.4 Privacy By Design

- 12.1.4.1 SKAO is committed to integrating Privacy by Design and Default into all processes, systems, and projects that involve the processing of personal data, as required under this ISMS Data Protection Policy. This means data protection will be considered at every stage of development, from initial planning to implementation and beyond. We will ensure that only necessary personal data is collected, processed, and retained, with appropriate technical and organizational measures in place to safeguard individuals' privacy. By ensuring that appropriate technical, organisational and privacy controls are in place, we aim to uphold the principles of privacy and data protection as a core priority in our operations. SKA Community Members that are developing applications will need to ensure Privacy by Design and Default and will be supported by the DPO on request.



12.1.5 Using Third Party Controllers and Processors

12.1.5.1 SKAO shall have a written contract, or other legal act, in place with each third-party processing SKAO Personal Data on its behalf.

12.1.5.2 SKAO contracts with Data Processors (or entities under the Australian Privacy Act 1988) shall describe:

- the subject matter and duration of the processing
- the nature and purpose of the processing
- the types and categories of Personal Data of Data Subjects
- the Data Controller's obligations and rights

12.1.5.3 The contract must contain specific clauses defining the responsibilities and obligations of both parties, including that:

- The Data Processor must only process Personal Data on SKAO's documented instructions, unless required by applicable law to process the Personal Data without such instructions;
- The Data Processor must ensure that all persons authorised to process Personal Data are subject to an appropriate duty of confidentiality;
- The Data Processor must implement appropriate technical and organisational measures to ensure the security of the processing;
- The Data Processor must not engage a sub-processor without SKAO's prior specific or general written authorisation. Where general written authorisation is provided, the Data Processor must inform SKAO of any intended changes concerning the addition or replacement of sub-processors and provide SKAO with an opportunity to object;
- Where a sub-processor is engaged, the Data Processor must impose data protection obligations on the sub-processor that provide an equivalent level of protection for Personal Data. The Data Processor remains responsible to SKAO for the compliance of its sub-processors with their data protection obligations;
- The Data Processor must take appropriate technical and organisational measures to assist SKAO in



responding to requests from Data Subjects exercising their data protection rights;

- Considering the nature of the processing and the information available, the Data Processor must assist SKAO in meeting its data protection obligations relating to the security of processing, Personal Data Breaches, Data Protection Impact Assessments
- The Data Processor must notify SKAO without undue delay after becoming aware of a Personal Data Breach and provide SKAO with the information and assistance required to meet its data protection obligations;
- The Data Processor must delete or return all Personal Data to SKAO, at SKAO's choice, at the end of the processing services and delete existing copies unless applicable law requires their continued storage; and
- The Data Processor must provide SKAO with all information necessary to demonstrate compliance with its obligations and allow for and contribute to audits and inspections conducted by SKAO or an auditor appointed by SKAO.

12.1.5.4 SKAO may require specific technical and organisational security measures to be defined within contracts, considering the nature and risks of the processing.

12.1.5.5 Contracts must include requirements relating to SKAO's privileges and immunities and the inviolability of its Data, where applicable.

12.1.5.6 As a Data Controller, SKAO shall only appoint Data Processors that can provide sufficient guarantees that they will implement appropriate technical and organisational measures to ensure that processing complies with applicable data protection requirements and protects the rights of Data Subjects. SKAO shall assess the suitability and reliability of Data Processors before appointing them and periodically as appropriate.

12.1.5.7 The SKAO Legal Team and DPO must be involved in reviewing and approving contracts with third parties relating to the processing of Personal Data on behalf of SKAO.



12.1.6 Data Protection Officer Responsibilities

12.1.6.1 The SKAO has appointed a Data Protection Officer (performing a role comparable to a Privacy Officer in Australia and an Information Officer under POPIA) to ensure compliance with this Data Protection Policy and its obligations to protect Personal Data collected from Data Subjects. The DPO must be involved in all issues which relate to the protection of Personal Data. The DPO responsibilities and tasks are outlined below:

- Providing information and advice relating to the SKAO's data protection obligations
- Reviewing and updating data protection policies and procedures to ensure they align with data protection legislation
- Monitoring the SKAOs compliance with this Data Protection Policy
- Providing advice and reviewing Data Protection Impact Assessments
- Maintaining the SKAO *Personal Data* assets register
- Providing data protection training
- Acting as a contact point for *Data Subjects*
- Ensuring *Data Subject* access requests are handled appropriately
- Verifying the legitimate basis for *processing Personal Data* and reviewing the adequacy of privacy notices
- Reviewing and approving contracts with third parties that process *Personal Data* on behalf of SKAO to ensure appropriate data protection requirements are included, with assistance from the Legal Team

12.1.7 SKA Community Member Responsibilities

12.1.7.1 SKA Community Members are responsible for ensuring that such processing is carried out appropriately, securely and transparently, and in accordance with this Policy, and that they can demonstrate compliance with its requirements.

12.1.7.2 SKA Community Members must understand their responsibilities and take appropriate action to ensure SKAO meets its data protection obligations as defined within this Policy.

12.1.7.3 These responsibilities include:

- Ensuring that all data *processing* activities comply with this Policy and are justified



- The ability to demonstrate compliance with this Policy, including creating and maintaining appropriate documentation to justify the *processing*
- Documenting and providing evidence of consent where necessary
- Working with the IT Team and DPO to ensure the appropriate technical and security measures have been implemented for new and existing *IT Systems* containing *Personal Data*
- Informing the DPO of all *Personal Data processing* activity so it can be added to the register of SKAO *Personal Data* assets, including reporting any changes to data *processing* activities
- Working with the DPO to maintain up to date and relevant documentation on all *processing* activities
- Assisting the DPO during the creation, review, and updates of privacy notices
- Being honest and transparent with the DPO during data protection compliance audits
- Completing Data Protection Impact Assessments where appropriate
- Maintaining the confidentiality of *Data Subjects* unless required by law, or during the proper performance of their duties
- Not *processing* or storing *Personal Data* in an unlawful or unauthorised manner
- Ensuring the SKAO is not placed at risk of compromise, including causing potential data breaches or reputational damage, due to their actions or inactions
- Following SKAO incident reporting policies and procedures [AD2] to report any concerns, suspicious activities, data breaches, errors, or non-compliance of this Policy without delay



12.1.8 Data Protection Training

12.1.8.1 SKAO shall ensure that all Staff Resources and Associates who are responsible for the collection, processing, storage, and removal of Personal Data receive the appropriate data protection training. This training will occur:

- During induction of Staff Resources and Associates
- At least every two years or whenever there is a substantial change in Policy

12.1.8.2 The DPO will arrange, monitor, and maintain data protection training records.

12.1.9 Monitoring

12.1.9.1 SKAO shall monitor its compliance with this Policy by conducting the following activities every two years:

- Conducting a data protection assessment to ensure compliance with this Policy and associated procedures [AD4]
- Conducting technical audits to ensure the effectiveness of the security controls in place [AD4]

12.1.10 Consequences of Failing to Comply

12.1.10.1 SKAO takes compliance with this Policy very seriously. Failure to comply puts both the SKA Community Members and SKAO at risk of reputational damage and mistrust.

12.1.10.2 Due to the importance of this Policy, failure to comply with any requirement may lead to disciplinary action which may result in dismissal. Where the individual is not an employee of SKAO, failure to comply may result in disabled access and/or a contractual review.



13 Notification of Personal Data Breaches

- 13.1 SKAO, as an intergovernmental organisation, is not required to report breaches of Personal Data to any official supervisory authority. However, SKAO shall inform the SKAO Council where a breach poses significant risk to the rights and freedoms of the affected Data Subjects upon discovery. The SKAO Council is the SKAO’s governing body and is comprised of representatives from each Member State. The SKAO Council is responsible for providing direction and authorisation concerning the response to and consequences of such breaches. All other data protection breaches shall be addressed in line with SKAOs security incident policies and procedures [AD2].
- 13.2 Where a breach occurs at a Data Processor acting on behalf of SKAO, the Data Processor must report the breach to SKAO upon discovery or within the agreed time period. SKAO shall respond to the breach in line with its policies and procedures. SKAO shall be responsible for informing the affected Data Subjects.
- 13.3 If there is a security incident that resulted in a data breach of our collaboration partners personal data, we will inform them within 24 hrs.
- 13.4 Where a SKA Community Member discovers an actual or potential breach of Personal Data, they must inform the IT Team or their SKAO Sponsor, in line with SKAO security incident reporting policies and procedures [AD2], and the DPO as soon as practically possible upon discovery.



13.5 All Personal Data breaches must be recorded and escalated in line with SKAO security incident policies and procedures [AD2].

14 Notification to the SKAO Council

14.1 SKAO Council must be informed where a breach poses significant risk to the rights and freedoms of the affected Data Subjects. Such breaches must follow the escalation process defined within the SKAO security incident reporting policies and procedures [AD2] and reported to the SKAO Council via the Director-General or their nominated deputy as soon as practically possible upon discovery.

14.2 The notification to the SKAO Council shall include:

- A description of the nature of the Personal Data breach, including the categories of Personal Data, the number of affected Data Subjects, and the number of records concerned
- A description of the likely consequences of the breach for the affected Data Subjects and SKAO
- A description of the measures taken or proposed to be taken to address the breach, including any measures to mitigate its possible adverse effects

15 Notification to the Data Subject

15.1 Where a Personal Data breach is likely to result in a high risk to the rights and freedoms of the affected Data Subjects, SKAO shall communicate the Personal Data breach to the affected Data Subjects as soon as practically possible upon discovery.

15.2 The communication to the affected Data Subjects shall be clear and in plain language and shall include:

- A description of the likely consequences of the breach
- A description of the measures taken or proposed to be taken to address the breach, including any measures to mitigate its possible adverse effects
- Any recommended measures to be taken by the Data Subjects to mitigate any adverse effects of the Personal Data breach



- The name and contact details of the DPO or other contact point where more information can be obtained

15.3 The Director-General, or their nominated deputy, must authorise any communication to affected Data Subjects if the data breach is likely to result in a high risk to their rights and freedoms.

15.4 The communication to the Data Subject is not required if one of the following conditions are met:

- SKAO has implemented appropriate technical or organisational measures that render the affected Personal Data unintelligible to unauthorised persons or prevent the identification of Data Subjects without access to additional information held separately, such as through encryption or effective pseudonymisation.
- SKAO has taken subsequent measures which ensure the high risk to the rights and freedoms of the affected Data Subjects is no longer likely to materialise
- It would involve disproportionate effort. In such cases SKAO shall submit a public communication or similar measure where Data Subjects are informed

15.5 SKAO may choose to communicate low or medium risk breaches to impacted Data Subjects with the documented authorisation of an Executive Group member.

16 Definition of Terms

Affiliate: is defined as an individual who does not have an employment relationship with the SKA Observatory, but who may require limited or specific access to SKAO IT Systems and information in order to complete their duties/role.

Asset is defined in this Policy as anything owned by the SKAO that must be protected from theft, compromise, or breaches of security. It can be a file, network service, system resource, process, product, IT infrastructure, database, intellectual property, personnel, personnel records, software, removable media, smartphone, certificates, cryptographic keys, etc.



Affiliate Contractor is defined as an individual working for the SKAO Observatory, under an agreed service contract for a specified period, and with limited or specific access to SKAO IT systems for the purpose of that contract.

Associate is defined as those who have signed an SKAO Associates contract with the SKA Observatory. Individuals are asked to sign an Associates contract when their involvement in SKAO is critical, or they have administrative access to systems as part of their role.

Data Subject is defined in this Policy as a natural or legal person, public authority, agency, or other body which processes Personal Data on behalf of the Data Controller

Data Subject is defined in this Policy as a natural living person, who can be identified directly or indirectly, whose Personal Data is collected, held, and, or processed. This is the equivalent of an 'Individual' as defined in the Australian Privacy Act 1988.

Information is defined in this Policy as physical or electronic documents and data stored within a database or information system.

IT Systems are defined in this Policy as physical IT equipment, information systems, control and monitoring systems, networks, and cloud resources, including any data they may contain.

Personal Data is defined in this Policy as any information relating to an identified or identifiable Data Subject. This is the equivalent of 'Personal Information' as defined in the Australian Privacy Act 1988. Personal Data includes, but is not limited to, the following:

- In the UK, Personal Data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- In South Africa, Personal Data also includes education, financial, and employment information, plus email address, physical address, and telephone number as Persona Data



- Both South African and Australian data protection laws, with which we align, define opinions about a Data Subject as personal data.

Processing is defined in this Policy as any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Secondees are defined in this Policy as an individual who is temporarily assigned to work at the SKA Observatory, but who continues to be employed by another organisation.

SKAO Associate is defined as those who have signed an SKAO Associates contract with the SKA Observatory. Individuals are asked to sign an Associates contract when their involvement in SKAO is critical, or they have administrative access to systems as part of their role.

SKA Community defined as the collective group of individuals who share an interest in the work of SKA Observatory, the SKA Project, and who participate in that work. This includes, but is not limited to, all Staff Resources, Affiliates and Visitors.

SKA Community Members: Members of the SKA Community who process Personal Data under the authority of, SKAO.

SKAO Personnel: defined as both SKAO Staff and Collaboration Staff (SKAO Staff, CSIRO employed SKA Low Personnel and SARAO employed SKA-Mid Personnel)

SKAO Staff defined as Employees of, or Secondees to, the SKA Observatory (as defined in Article 1(k) of the Convention)

Staff Resources is defined as an individual working in a defined role within the SKA Observatory, such as an SKAO Employee, Collaboration Staff, Secondee, Studentship, and Staff Resource Contingent Worker.



A References

A.1 Applicable documents

The following documents are applicable to the extent stated herein. In the event of conflict between the contents of the applicable documents and this document, **the applicable documents** shall take precedence.

- [AD1] SKAO-GOV-0000011 Information Security Scope
- [AD2] Australian Privacy Applicability Document [TBC]
- [AD3] South African Privacy Applicability Document [TBC]
- [AD4] SKAO-GOV-00000144 Incident Response Procedure
- [AD5] SKAO-GOV-0000010 Information Security Policy
- [AD6] SKAO-GOV-0000005 Information Classification, Labelling and Handling
- [AD7] SKAO-GOV-00000127 Access Control and Physical Security
- [AD8] SKAO-GOV-0000167 Data Retention
- [AD9] SKAO-GOV-00000268 Data Retention Schedule
- [AD10] SKAO-GOV-0000019 Information Security in Supplier Relationships
- [AD11] SKAO-GOV-0000023 Risk Assessment Methodology
- [AD12] SKAO-GOV-000002 Network and Operational Security
- [AD13] SKAO-GOV0000166 Artificial Intelligence
- [AD14] SKAO-GOV-0000018 Security Requirements of Information Systems
- [AD15] SKAO-GOV-0000014 Acceptable Use
- [AD16] SKA Community Acceptable Use [TBC]

A.2 Reference documents

The following documents are referenced in this document. In the event of conflict between the contents of the referenced documents and this document, **this document** shall take precedence.

- [RD1] ISO 27001:2013 Information Security Management System Requirements



LIST OF ABBREVIATIONS

IGO.....	Inter-Governmental Organisation
ISMF	Information Security Management Forum
ISMS.....	Information Security Management System
ISO.....	International Standards Organisation
IT	Information Technology
NREN	National Research and Education Network
POP	Point of Presence
PV	Photovoltaic (Solar Power Plant)
SKA	Square Kilometre Array
SKAO	Square Kilometre Array Observatory
SRC	SKA Regional Centre

POLICY APPROVAL AND OWNERSHIP DETAILS

POLICY APPROVAL AND OWNERSHIP DETAILS	
Impact Assessment:	Yes
Date of Review:	2025-12-02
Reviewer:	Debbie McLachrie
Document Location:	[Path link]
Compliance Checks:	Yes

DOCUMENT HISTORY

Revision	Date Of Issue	Comments
A	2015-12-02	First draft release for internal review
B	2016-01-20	Updated post Security Workshop
C	2018-07-20	Modified the responsibilities paragraph of the Executive Summary to align with other policy documents. Updated the



		Intended Audience section. Re-wrote Section 4, as the design has evolved significantly since the previous version of this document.
D	2018-11-08	Converted the document to the latest document template. Removed the reference to the ISMS Statement of Applicability document, as it is no longer referenced in this document. Added a statement regarding the IGO status and the storage of SKA Observatory data in the cloud.
E	2020-01-16	Document has been reviewed for accuracy and relevance as part of an annual review. Corrected the name of this document. Added [RD2] and referenced it within this document. Added "Global" to Headquarters in Table 1. Included information systems to the sentence regarding documentation containing SKA information. Updated the Cloud Provider paragraph in section 3 to emphasise that there will be more than one provider. Updated the SRC paragraph in section 3.
01	2020-01-16	This document is ready to be reviewed by the Senior Leadership Team.
01A	2020-06-10	Transferred policy text to new document template. Included comments received from Colin Greenwood and Simon Berry.
02	2020-07-16	Implemented the comments from the reviewers. Reworded some of the Introduction section to ensure clarity. Amended small amounts of text throughout the document to improve the clarity, the general concepts remain unchanged. Updated Section 5 to include the definition of IT systems.
02A	2021-10-28	Migrated to SKAO policy template. Updated all sections to ensure accuracy and relevance as part of the annual review.
02B	2022-01-05	Applied generic changes and prepared document for IPG review.
03	2022-02-25	Policy reviewed by the IPG and released.
04	2025-12-02	Widened the scope to include Community Members who process SKAO data, added



		some missing elements (archiving, marketing, sensitive cultural data handling, privacy by design), updated relevant sections in line with the DUAA, documented further information about international transfers.
--	--	---

ORGANISATION DETAILS

Name	SKA Observatory
Registered Address	Jodrell Bank Lower Withington Macclesfield Cheshire, SK11 9FT, UK
Fax	+44 (0)161 306 9600
Website	www.skao.int

