RioTinto

Data Privacy Standard

GOV-B-003

Group:	**Function:**	**No. of Pages:**
Mandatory for all Rio Tinto staff and each Rio Tinto Group Business and Function	Group Ethics & Compliance	10

Reviewed:	**Effective:**	**Auditable From:**
September 2021	1 February 2022	1 February 2023

Supersedes: 2018 Data privacy standard

Owner:	**Approver:**	**Target Audience:**
Chief Ethics & Compliance Officer	Executive Committee	All employees and core contractors. Core contractors refers to category 1 and category 2 contractors and any external processors, subprocessors, consultants and other service providers who perform internal duties or roles that involve personal data processing of any kind, or that have access to internal Rio Tinto systems

Direct linkages to other relevant policies, standards, procedures or guidance notes:

- The way we work
- Group Standard on Acceptable Use of Information and Electronic Resources
- Group Procedure on Information and Cyber Security
- Records Management Standard and the Records Retention and Disposition Schedule

Document purpose:

- Rio Tinto has obligations under privacy and data protection (data privacy) laws around the world. The Data Privacy Standard establishes minimum requirements for the processing of personal data across Rio Tinto's global operations. This not only assists Rio Tinto to comply with its data privacy obligations wherever and whenever it processes personal data, it also aims to maintain the trust of people who share their personal data with Rio Tinto.
- The Data Privacy Standard also operates as Rio Tinto's 'privacy policy' wherever an organisation-wide privacy policy is required under applicable data privacy laws.

Data Privacy Standard

Introduction
What does this Standard do?

The *Data Privacy Standard* sets out the minimum rules (**Data Privacy Principles**) that apply whenever and wherever Rio Tinto collects and **processes personal data** in any format, including electronic and paper. The Data Privacy Principles reflect the benchmark for processing **personal data** across the Rio Tinto Group. Note that:

- **personal data** means all information relating to any identifiable individual.
    - For example, **personal data** includes professional contact details, photographs, information about an individual's activities or their characteristics. However, **personal data** does not include information that cannot be associated to an identifiable individual either directly or indirectly (taking into account the means reasonably likely to be used to make such an association, as well as the costs and the amount of time required and the available technologies).
- **process** and processing cover everything we might do with **personal data**.

The Glossary at the end of the Standard defines these and other terms (indicated in **bold**) that are used in this Standard.

Who does this Standard apply to?

This Standard applies to everyone who works for Rio Tinto, and to each Rio Tinto **Group business**.

Why is compliance with this Standard important?

At Rio Tinto, the lawful and correct handling of **personal data** is critical. At its simplest, people need to be able to trust us to respect their privacy and how we handle their **personal data** when working with us or doing business with us.

In addition, we need to comply with privacy and data protection laws around the world. Applying the **Data Privacy Principles** in this *Data Privacy Standard* helps us to do this. Failure to comply with these principles could lead to financial and reputational damage to Rio Tinto, as well as resulting in a loss of trust from the individuals we employ, engage or do business with.

What do we need to comply with?

These Data Privacy Principles create a global standard which helps Rio Tinto ensure that we act consistently with our obligations under the many different local data privacy laws around the world.

We must comply with these **Data Privacy Principles** and with any additional requirements under local data privacy laws that apply to the **processing** of **personal data**. If there is a conflict between the requirements under the **Data Privacy Principles** and local data privacy laws, you should comply with the most stringent requirement.

Any variance from or exception to the Data Privacy Standard must be approved by the Chief Ethics & Compliance Officer. This Standard will be reviewed at least once every three (3) years.

Data Privacy Control

Any proposed **personal data processing** that can potentially lead to **data subject** complaints, regulatory investigations, enforcement actions or damage to Rio Tinto's reputation must be subject to a Privacy Impact Assessment (PIA) from Ethics and Compliance. The Chief Ethics and Compliance Officer may suspend or block proposed **personal data processing** activities that, as assessed by Ethics and Compliance, represent a high risk of producing complaints, regulatory investigations, enforcement actions or which could damage Rio Tinto's reputation.

Data Privacy Principles

The following **Data Privacy Principles** reflect the minimum rules that apply to the **processing** of **personal data** at Rio Tinto.

Data Privacy Principle 1: Our processing of personal data is lawful, fair and transparent

- **Lawful basis for processing:** We will only **process personal data**:
  - for a **legitimate business purpose** we collected it for, as notified in a **privacy statement**;
  - for other purposes that the **data subject** (the person that the data relates to) **consents** to;
  - where necessary for the performance of a contract with the **data subject**;
  - if the **processing** is required in order to comply with our legal obligations; or
  - if the **processing** is expressly permitted under local data privacy laws and the relevant **personal data** originates in that jurisdiction.

  Appendix 1 provides an overview of the purposes for which Rio Tinto undertakes personal data processing.
- **Notification of processing:** We will notify **data subjects** that we're collecting their **personal data**, by providing a **privacy statement** at or before the time we collect **personal data** from them.
- **Collections by or from third parties:** Where **personal data** has been collected by or from third parties, we will ensure that the **personal data** is lawfully disclosed to us. This includes confirming that **data subjects** were notified and that a lawful basis exists for the disclosure. We will only **process** the **personal data** as permitted by applicable data privacy laws.

Data Privacy Principle 2: We limit our personal data processing

- **Purpose limitation:** Our **personal data processing** must be for specific and limited purposes, as notified to the **data subject**.
- If we **process personal data** for a different purpose than that notified, we need to inform the relevant **data subject**(s) of that new purpose (in accordance with Data Privacy Principle 1) and confirm that:
  - the **data subject** consents to the **processing** of his or her **personal data** for this new purpose;
  - the **processing** is required to comply with an applicable law;
  - the new purposes for **processing** the personal data are compatible with the original **processing** purposes; or
  - the **processing** otherwise is lawful under applicable data privacy laws.

  Processing for a new purpose will only be found to be compatible with the original purpose where applicable law so provides, or we have assessed and concluded that it is taking into account such

factors as the relationship between the initial purposes and the new purpose; the context in which the **personal data** was collected and expectations of **data subjects**; the nature of the **personal data**; the consequences of the new **processing** for **data subjects**; and whether there are privacy safeguards in place.

- **Data minimisation:** We must **process** only that amount of **personal data** that we need for the relevant **processing** purpose, and only to the extent necessary for that purpose. Our **Personal data processing** must be adequate, relevant and not excessive.

Data Privacy Principle 3: We maintain data quality

When we **process personal data**, we take reasonable steps to ensure that:

- **personal data** is accurate and where necessary, is kept up to date; and
- if **personal data** is needed to make decisions about a data subject but is inaccurate, such **personal data** is erased, rectified or supplemented (having regard to the processing purpose).

Data Privacy Principle 4: We are careful with sensitive information

Sensitive information is a type of **personal data** that is of a particularly private nature and includes (among other things) **personal data** about a person's race, ethnic origins, trade union membership and health and biometric information, as well as **criminal-record information**. We must ensure that **sensitive information** is **processed** only when necessary and only if:

- the **data subject consents**; or
- if **processing** is:
    - required in order to comply with our legal obligations,
    - is expressly permitted under local data privacy laws or local labour laws and the relevant **personal data** originates in that jurisdiction; or
    - necessary to prevent or lessen a serious and imminent threat to the life, health or safety of any person.

Data Privacy Principle 5: We protect our disclosures of personal data

We protect **disclosures** of **personal data** (including but not limited to when it is transferred across national borders) as follows:

- **Disclosures outside the Rio Tinto Group:** If we need to disclose **personal data** outside the **Rio Tinto Group** (for example, to an external service provider or to a third party who is authorised to receive the **personal data**), we must ensure that:
    - the **disclosure** is protected by contractual data privacy clauses approved by Ethics & Compliance or Rio Tinto Legal. This must include an assessment of whether any transfers across national borders comply with applicable data privacy laws (see requirements in Appendix 2b);
    - the relevant **data subjects** have **consented** to the **disclosure**; or
    - the **disclosure** is otherwise required by law or is or is expressly permitted under local data privacy laws and the relevant **personal data** originates in that jurisdiction.
- **Disclosures within the Rio Tinto Group: Disclosures** within the **Rio Tinto Group** are protected by the **Rio Tinto Data Transfer Deed** if it is necessary to share **personal data** outside of the jurisdiction where the **personal data** was first collected. Company secretarial and each **Group business** will ensure that any new Group companies sign up to the **Rio Tinto Data Transfer Deed**.

An overview of international disclosures/transfers (both within the Rio Tinto Group and to external service providers) is at Appendix 2a.

Data Privacy Principle 6: We must secure personal data

- **General data security obligations: Personal data** must be kept secure and protected against accidental, unauthorised or unlawful **processing**, including against loss and unauthorised access, destruction, misuse, modification or **disclosure**. This means ensuring that Rio Tinto has appropriate technical and organisational measures in place. Data security obligations apply whether **personal data** is stored in hard copy form (eg paper) or in electronic form (eg in databases). The key rules are:
    - access to **personal data** about other people should be on a "need to know" basis only; and
    - each **Group business** must implement the Rio Tinto Group Standard on Acceptable Use of Information and Electronic Resources and the Group Procedure on Information and Cyber Security (administered by Cyber Security in IS&T) to ensure that appropriate physical, technical and organisational security measures are in place at all stages of the **personal data** 'life cycle'.
- **Internal reporting of Data Privacy Incidents:** Each **Data Privacy Incident** must be immediately reported to Ethics and Compliance. Where required by applicable data privacy laws, Ethics & Compliance will ensure that a **data breach** is notified to the competent authority(ies) and affected **data subjects**.

Data Privacy Principle 7: We limit retention of personal data

Personal data must be kept only for as long as necessary for the lawful purpose for which it is **processed** (as notified to the relevant individuals), or for the time required or permitted under local laws (whichever is the shorter). **Personal data** will be retained in accordance with the Records Retention and Disposition Schedule (made under the Rio Tinto Records Management Standard and as updated from time to time), which sets out periods for which different types of records containing personal data are needed. After such time, records containing **personal data** must be securely destroyed (in the case of physical records) or permanently deleted (in the case of electronic records) in accordance with Rio Tinto's Records Retention and Disposition Schedule or applicable local laws (whichever imposes the strictest obligations). To the extent possible, all archived copies and back-up copies should be destroyed at the same time and in the same manner as any original records that contain the **personal data**.

Data Privacy Principle 8: We respect data subject rights

Data subjects have the right to:

- seek access to **personal data** that Rio Tinto holds about them;
- seek correction of inaccurate, incomplete or out of date **personal data**;
- seek erasure of their **personal data**;
- be provided with information about how their **personal data** is **processed**;
- ask for **processing** of their **personal data** to cease (particularly if the **processing** is likely to cause damage or distress, or if the **processing** is for direct marketing purposes);
- be notified if the **Group business** has made a decision about the **data subject** that is based on automated data **processing** alone (so that the **data subject** can ask for a review of the decision, if necessary);
- complain about the **processing** of their **personal data;** or
- withdraw previously given **consent** regarding Rio Tinto's **processing** of their **personal data.**

There are legal exceptions to the exercise of these rights, and Rio Tinto will review each request on a case by case basis, by reference to the laws of the country where the **data subject** is located (or if the country where the data subject is located has no data privacy laws, by reference to the data privacy laws in Australia). Requests from **data subjects** to access their rights should be notified to the **Data Privacy Lead** for the relevant region, who will advise on how the request needs to be responded to. Appendix 3 contains more information about how to exercise data privacy rights.

Data Privacy Principle 9: We apply privacy by design

We must ensure that data privacy compliance is integrated into our personal data processing activities.

Threshold Privacy Assessment:

Ethics & Compliance will undertake a Threshold Privacy Assessment if it is proposed to:

- introduce a new or expanded personal data processing technology or system;
- outsource personal data processing functions; or
- collect or generate new personal data categories, or to process existing personal data for a new purpose.

The Threshold Privacy Assessment will consider:

- the nature of the personal data;
- the proposed processing purpose;
- proposed disclosures of the personal data, including any proposed trans-border data flows.

This information will be collected as part of the Security Risk Assessment (**SRA**) process undertaken by Cyber Security, or separately by Ethics & Compliance.

Privacy Impact Assessment:

If the Threshold Privacy Assessment indicates that the proposed processing is likely to result in a high risk to the privacy rights of data subjects, Ethics & Compliance will conduct a Privacy Impact Assessment. The Privacy Impact Assessment will identify steps that must be taken to mitigate the risk and to ensure that Rio Tinto complies with its obligations under this Standard and applicable data privacy laws.

Data Privacy Principle 10: We don’t spam

We must limit our use of **personal data** to send **marketing communications**. All **marketing communications** (however distributed) must:

- clearly identify the relevant **Group business** or Group company as the sender, and how it can be contacted;
- be sent with the **consent** of the recipient/**data subject,** unless Ethics & Compliance has advised that consent is not required in the relevant country where the proposed recipients are located; and
- contain an unsubscribe or opt out facility. Opt outs must be acted upon and records amended accordingly.

Glossary

Consent of a **data subject** means any freely given, specific, informed and unambiguous indication of the **data subject**’s wishes.

Criminal record information means **personal data** relating to criminal convictions and offences.

Data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised **disclosure** of, or access to, **personal data** transmitted, stored or otherwise **processed**.

Data Privacy Incident means a **data breach** or a known or suspected breach of any of the other **Data Privacy Principles** in this Data Privacy Standard.

Data Privacy Lead means a member of Ethics & Compliance who is the first point of contact for data privacy questions from your region, as listed on the data privacy page on Element.

Data Privacy Principles means the principles in this Data Privacy Standard that Rio Tinto Group companies and staff must apply when **processing personal data**.

Data subject means the individual to whom **personal data** relates.

Disclosure means the act by which **personal data** is made accessible to others.

Group business includes all companies, product groups, business units, global functions and corporate offices in the Rio Tinto Group.

Legitimate business purpose means a purpose that is directed at Rio Tinto achieving its proper business objectives and that complies with all applicable laws and regulations, and with Rio Tinto's policies and standards.

Marketing communications means communications and publications that have a purpose of marketing or promoting Rio Tinto or its products, but does not include communications from Rio Tinto to its employees that relate to the administration of the employment relationship.

Personal data means all information relating to any identifiable individual.

Privacy Impact Assessment means an assessment of the impact of proposed **processing** operations on the rights and freedoms of **data subjects**, and the protection of **personal data**.

Privacy Statement means a notice that needs to be provided to **data subjects** when we collect their **personal data**.

Processing means all actions taken in relation to **personal data** including collecting, using, disclosing, recording, organising, storing, transferring, amending, deleting, destroying, retrieving, accessing, hosting or otherwise handling.

Rio Tinto Data Transfer Deed means the deed executed between Rio Tinto Limited and Rio Tinto plc on 1 July 2009 (as amended from time to time) and to which Rio Tinto Group companies are bound under executed Deeds of Accession.

Rio Tinto Group means all the businesses which are wholly or majority owned or managed by Rio Tinto plc or Rio Tinto Limited (whether directly or indirectly).

Sensitive information means **personal data** (including information or an opinion) about an individual's racial or ethnic origin, political opinions and memberships, religious or philosophical beliefs or associations, trade union membership, **criminal record information**, genetic data, biometric data (**processed** for the purpose of uniquely identifying a natural person), health or the health services they have received or details of sexual life.

Appendix 1
Overview of personal data collections and processing

Rio Tinto collects and **processes personal data** for a range of business purposes, including:

- Managing People data: **Personal data** about employees, prospective employees and contractors is collected for human resources (HR) purposes. This includes identity and contact information, data about employment history, training and qualifications, performance information and information needed to pay salaries and other benefits;
- Managing business relationships with customers, suppliers and other external parties (such as individuals within joint venture partners). **Personal data** about individuals within external organisations is collected for business purposes such as supplying goods or acquiring services, entering into and fulfilling contracts and for communications purposes. This is often limited to 'business contact' information;
- Managing shareholder relationships: **Personal data** from shareholders is collected for purposes related to their shareholding in Rio Tinto, including for the purposes of issuing or transacting in shares, paying dividends, regulatory reporting and shareholder communications. This **personal data** may include a shareholder's name, address, shareholding details, tax file number, and bank account details. Shareholder **personal data** is collected by Rio Tinto and our behalf by the external manager of our share register. From time to time this data may be provided to other external service providers for the purposes of paying distributions or mailing shareholder communications, or to the extent permitted by legislation to authorised securities brokers, persons inspecting the register, bidders for Rio Tinto's securities, or certain regulatory bodies including the Australian Taxation Office;
- Safety, security and legal obligations: **Personal data** is collected from visitors to our sites for safety and security purposes. This can include collection of images by closed circuit television (CCTV), where permitted under local laws. Rio Tinto also collects **personal data** in the course of complying with its legal obligations (for example, to meet obligations under anti-money laundering legislation and whistleblowing legislation); and
- Managing community relationships: **Personal data** is collected from members of communities where Rio Tinto conducts mining and other operations, for the purposes of engaging and interacting with those communities.

Rio Tinto collects **personal data** directly from **data subjects** wherever possible.

Personal data may be stored in Rio Tinto's local systems or databases, in the Rio Tinto Business Solution (a SAP system that is hosted in Australia), or on infrastructure owned and operated by external service providers engaged by Rio Tinto. Where external service providers are engaged to assist Rio Tinto to **process personal data**, Rio Tinto requires such service providers to comply with contractual privacy and data protection obligations and applicable data privacy laws.

Appendix 2
International disclosures

a. Overview of international disclosures

An overview of Rio Tinto's global operations and the countries where it operates is on the Rio Tinto website. This explains where each of the Rio Tinto product groups operates, on a "country by country" basis.

If you are employed or engaged by or have business dealings with a particular Rio Tinto product group, your **personal data** may be exchanged between Rio Tinto Group companies that are in the countries listed for that product group.

Also, your **personal data** may be **processed** by Rio Tinto "shared services" companies and external service providers that provide services to the Rio Tinto Group in one or more of the following countries:

- **Rio Tinto companies performing "shared services"** are located in the following countries: Australia, Canada, India, Mongolia, Singapore, South Africa, the United Kingdom and the United States.
- **External service providers** that assist the Rio Tinto Group to perform global HR and other shared service functions, and which **process personal data** on behalf of one or more companies in the Rio Tinto Group are located in: Australia, Canada, the European Union, India, Malaysia, the Philippines, Poland, the United Kingdom and the United States.

Shareholder **personal data** is **processed** in Australia and the United Kingdom by Rio Tinto and by the external manager of our share register.

b. Assessment prior to international disclosures

Prior to transferring **personal data** outside the country where it was collected, the relevant Group business will carry out the following assessment (with assistance from Ethics & Compliance):

- We will verify whether the **data subjects** were informed that their **personal data** will be transferred.
- We will verify whether the transfer is covered by onward transfer provisions or other provisions in Rio Tinto's inter-company agreement (the Rio Tinto Data Transfer Deed), or whether additional clauses are required.
- International transfers of **sensitive information** require review from Ethics & Compliance.
- For **disclosures** outside the Rio Tinto Group, we will ensure that the third party can ensure the security and privacy of the **personal data**. We may ask the third party to provide a description of the technical and organisational measures in place to protect the **personal data**. Rio Tinto's Cyber Security team will assess whether these measures are sufficient (eg as part of its Security Risk Assessment).

Appendix 3
Data subject rights and complaints

a. General data subject rights

Please complete a ***Data subject request form*** if you wish to exercise your rights under Data Privacy Principle 8, including to:

- seek access to **personal data** that Rio Tinto holds about you;
- seek correction or erasure of inaccurate, incomplete or out of date **personal data**;
- be provided with information about how your **personal data** is **processed**;
- subject to whether the right of 'data portability' is a right under the data privacy laws of your country, receive a copy of your **personal data** in a structured, commonly used and machine-readable format and request that we transmit personal data you provide to us to a third party;
- subject to whether the right to request cessation of processing is a right under the data privacy laws of your country, request **processing** of your **personal data** to cease on a temporary or permanent basis (e.g., if the accuracy of the **personal data** is contested or the **processing** is unlawful in your opinion, or if the **processing** is likely to cause damage or distress, or if the **processing** is for direct marketing purposes);
- seek information about or a copy of the mechanisms we use to transfer your **personal data**
- withdraw **consent** you have previously provided in relation to Rio Tinto's **processing** of your **personal data**.

Your request will be forwarded to the **Data Privacy Lead** for your region, who can also provide you with the *Data subject request form*. Rio Tinto will aim to respond within a reasonable period after the request is made or from when information required to **process** the request is received (or otherwise as required under local laws).

b. Questions or complaints

If you have any questions or wish to make a complaint about the **processing** of your **personal data**, you can do so by emailing aske&C@riotinto.com or by reporting this as a **Data Privacy Incident** to Ethics & Compliance.

Data Privacy Leads are responsible for investigating and responding to complaints, unless the complaint is about the **Data Privacy Lead**'s **processing** of **personal data**. In such circumstances, another person will be appointed to investigate and respond to the relevant complaint. If you are not satisfied with how your complaint has been addressed, complaints may be made to, where available, the relevant data privacy regulator or data protection authority in your country.