RioTinto

Group Standard Mandatory for all Rio Tinto staff and each Rio Tinto Group Business and Function	Title: **Data Privacy Standard**		
	Function: **Group Ethics & Integrity**		
	No. of Pages: **9 (5 + Title Page + Appendices)**		
	Reviewed: **November 2017**	Effective:	Supersedes: **2014 Data privacy standard**
Owner: **Head of Ethics & Integrity**		Approver: **Executive Committee**	

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. 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.
- **process** and **processing** covers everything we might do with **personal data**.

The Glossary at the end of the Standard defines these and other terms used in this Standard (in **red**).

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?

We must comply with the **Data Privacy Principles** and also with local laws that apply to the **processing** of personal data. If there is a conflict between the requirements under the **Data Privacy Principles** and local laws, you should comply with the most stringent requirement. Please note that the Country Supplements on the data privacy page on Element provide an overview of relevant additional requirements under local data privacy laws of some Rio Tinto operating countries.

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

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 the **legitimate business purpose** we collected it for, as explained 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.

- **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.

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).
- **Data minimisation:** We must process only that amount of **personal data** that we need for the relevant processing 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 the **personal data** is accurate and where necessary, is kept up to date.

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 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 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 & Integrity or Rio Tinto Legal. This must include an assessment of whether any transfers across national borders comply with applicable data privacy laws;
  - 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**.

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:** **Data Privacy Incidents** are Group reportable incidents under the Investigations Procedure. Each **Data Privacy Incident m**ust be immediately reported to Ethics and Integrity.

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). 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 Procedure or applicable local laws (whichever imposes the strictest obligations).

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. Requests from data subjects to access their rights should be referred to the **Data Privacy Lead** for the relevant region.

Data Privacy Principle 9: We apply Privacy by Design

We must:

- integrate data privacy compliance measures into our **personal data processing** activities; and
- consider individual privacy rights from the outset of each new **personal data processing** activity.

We will undertake a **Privacy Impact Assessment** when we introduce a new **personal data processing** technology, or whenever new **personal data processing** or changes to existing **personal data processing** is likely to result in a risk to the rights of **data subjects**.

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** (which may be able to be implied from an existing business relationship or shareholding); 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.

Data Privacy Incident means a known or suspected breach of:

- the data security obligations in Data Privacy Principle 6; or
- any of the other **Data Privacy Principles** in this Data Privacy Standard.

Data Privacy Lead means a member of Ethics & Integrity 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: the principles in the *Data Privacy Standard* that Rio Tinto Group companies and staff must apply when processing personal data.

Data subject: the individual to whom personal data relates.

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

Legitimate business purpose: a purpose that is directed at Rio Tinto achieving its business objectives and that complies with all relevant laws and regulations.

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: 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: a notice that needs to be provided to data subjects when we collect their personal data.

Processing: 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: 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: 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: 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, 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 human resources: **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. **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 usually 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

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 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, 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.

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; or
- request processing of your **personal data** to cease (eg if the processing is likely to cause; damage or distress, or if the **processing** is for direct marketing purposes); or
- 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. Complaints

If you wish to make a complaint about the **processing** of your **personal data**, you can do so by emailing compliance6@riotinto.com or by reporting this as a **Data Privacy Incident** to Ethics & Integrity.

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.