

Norme de confidentialité des données

GOV-B-003

Groupe : Obligatoire pour tout le personnel Rio Tinto et toutes les unités et fonctions du Groupe Rio Tinto	Fonction : Groupe éthique et conformité	Nbre de pages : 11
Révision : Septembre 2021	Date d'entrée en vigueur : 1 février 2022	Vérifiable à partir du : 1 février 2023
Remplace : Norme de confidentialité des données 2018		
Propriétaire : Directeur Éthique et Conformité	Approbateur : Comité exécutif	Public cible : Tous les salariés et prestataires principaux. L'expression « prestataires principaux » se rapporte aux prestataires de catégories 1 et 2 et à tout sous-traitant, consultant et autre prestataire de service externe qui réalise des activités ou exerce un rôle en interne impliquant un traitement de données personnelles, ou a accès aux systèmes internes de Rio Tinto de par ses fonctions.

Liens directs avec d'autres politiques, normes, procédures ou notes d'orientation pertinentes :

- Notre approche de l'entreprise
- Norme du Groupe relative à une Utilisation acceptable des informations et des ressources électroniques
- Procédure du Groupe relative à l'Information et la cybersécurité
- Norme de gestion des dossiers et Calendrier de rétention et de destruction des dossiers

Objectif du document :

- Rio Tinto a des obligations en vertu des différentes lois sur la confidentialité des données personnelles dans le monde. La Norme de confidentialité des données établit les exigences minimales en matière de traitement des données personnelles pour toutes les opérations de Rio Tinto à travers le monde. Elle permet non seulement à Rio Tinto de se conformer à ses obligations en matière de confidentialité des données chaque fois qu'il recueille et traite des données à caractère personnel, elle vise également à conserver la confiance des personnes qui communiquent leurs données personnelles à Rio Tinto.
- La Norme de confidentialité des données fait également office de « Politique de confidentialité » de Rio Tinto chaque fois qu'une politique de confidentialité est requise à l'échelle de toute l'entreprise, en vertu des lois en vigueur sur la confidentialité des données.

Norme de confidentialité des données

Introduction

En quoi consiste cette norme ?

La *Norme de confidentialité des données* stipule les règles minimales (**principes de confidentialité des données**) qui s'appliquent chaque fois que Rio Tinto recueille et **traite des données à caractère personnel**, sous quelque format que ce soit, y compris électronique et papier.

Les **principes de confidentialité des données** servent de référence pour le traitement des données à caractère personnel dans l'ensemble du groupe Rio Tinto. On retiendra les termes clés suivants :

- le terme « **données à caractère personnel** » signifie toute information relative à une personne physique identifiable.
 - Par exemple, le terme « **données à caractère personnel** » couvre les coordonnées de contact, photographies et informations relatives aux activités ou aux caractéristiques d'une personne physique. Le terme « **données à caractère personnel** » ne couvre cependant pas les informations qui ne peuvent pas être associées à une personne physique identifiable, que ce soit directement ou indirectement (en tenant compte des moyens raisonnablement susceptibles d'être utilisés pour une association de ce type, ainsi que des coûts et du temps nécessaires et des technologies disponibles).
- les termes « **traiter** » et « traitement » englobent toute opération portant sur des **données à caractère personnel**.

Le Glossaire situé à la fin de la présente Norme définit ces termes et d'autres termes qui y sont utilisés (en caractères **gras**).

À qui s'adresse cette norme ?

La présente norme s'applique à quiconque travaille pour Rio Tinto ainsi qu'à chaque **entité du groupe**.

Pourquoi respecter cette norme ?

Chez Rio Tinto, nous considérons qu'il est essentiel d'assurer un traitement légal et adéquat des **données à caractère personnel**. Autrement dit, les personnes qui travaillent ou qui font affaire avec nous doivent pouvoir compter sur notre capacité à respecter leur vie privée et à traiter leurs **données à caractère personnel** en toute sécurité.

En outre, nous devons respecter les lois sur la confidentialité et la protection des données dans le monde entier. L'application des **Principes de confidentialité des données** énoncés aux présentes nous le garantit. Le non-respect de ces principes pourrait entraîner des dommages financiers et une atteinte à la réputation de Rio Tinto, et entraîner une perte de confiance de la part des personnes que nous employons, avec lesquelles nous sommes en contact ou avec lesquelles nous faisons affaire.

Quelles exigences de conformité devons-nous respecter ?

Ces Principes de confidentialité des données créent une norme internationale qui permet à Rio Tinto de s'assurer qu'il respecte ses obligations en vertu des différentes lois locales sur la confidentialité des données à travers le monde.

Nous devons nous conformer aux **principes de confidentialité des données**, de même qu'aux lois locales relatives au **traitement des données à caractère personnel**. En cas de conflit entre les exigences des **principes de confidentialité des données** et celles des lois locales sur la confidentialité des données, il convient d'adopter les dispositions les plus strictes.

Tout écart ou dérogation par rapport à la Norme de confidentialité des données doit être approuvé par le Responsable Éthique et intégrité. La présente norme sera révisée une fois tous les trois ans au moins.

Contrôle de la confidentialité des données

Tout **traitement de données à caractère personnel** proposé susceptible de générer des plaintes de la part de la **personne concernée**, des enquêtes réglementaires, des mesures coercitives ou de porter atteinte à la réputation de **Rio Tinto** doit être soumis à une Évaluation d'impact sur la vie privée de la part du département Éthique et Conformité. Le Directeur Éthique et Conformité peut suspendre ou bloquer des activités de **traitement de données à caractère personnel** proposées si, après évaluation par le département Éthique et Conformité, elles présentent un risque élevé de générer des plaintes, des enquêtes réglementaires, des mesures coercitives ou de porter atteinte à la réputation de Rio Tinto.

Principes de confidentialité des données

Les **principes de confidentialité des données** suivants stipulent les règles minimales applicables au **traitement des données à caractère personnel** chez Rio Tinto.

Principe 1 de confidentialité des données : le traitement des données à caractère personnel que nous effectuons est licite, équitable et transparent

- **Base légale du traitement** : Nous traiterons les **données à caractère personnel** uniquement :
 - aux **finals commerciales légitimes** pour lesquelles nous les avons recueillies, comme spécifié dans la **déclaration de confidentialité** ;
 - aux autres fins auxquelles **consent** la **personne concernée** (la personne à laquelle se rapportent les données à caractère personnel) ;
 - lorsque le traitement est nécessaire à l'exécution du contrat qui le lie à la **personne concernée** ;
 - si le **traitement** est requis par Rio Tinto pour respecter ses obligations légales ; ou
 - si le **traitement** est expressément autorisé par les lois locales sur la confidentialité des données personnelles et si les **données à caractère personnel** concernées proviennent de ce territoire.

L'annexe 1 fournit un aperçu des finalités pour lesquelles Rio Tinto traite des données à caractère personnel.

- **Notification des traitements** : Nous informerons les **personnes concernées** que nous recueillons leurs **données à caractère personnel** en leur transmettant une **déclaration de confidentialité** au moment de la collecte ou immédiatement après celle-ci.
- **Collecte par ou auprès de tierces parties** : Lorsque des **données à caractère personnel** ont été recueillies par ou auprès de tierces parties, nous veillerons à ce que les **données à caractère personnel** nous soient divulguées en toute légalité. Ceci comprend la confirmation que les **personnes concernées** ont été notifiées et qu'il existe une base légale pour la divulgation. Nous **traiterons** les **données à caractère personnel** uniquement si cela est autorisé par les lois en vigueur sur la confidentialité des données.

Principe 2 de confidentialité des données : nous limitons l'utilisation des données à caractère personnel

- **Limitation de la finalité** : Le **traitement des données à caractère personnel** que nous

effectuons doit viser des finalités précises et limitées, dont la **personne concernée** est informée.

- Si nous **traitons des données à caractère personnel** à des fins différentes de celles qui sont annoncées, nous devons informer la ou les **personnes concernées** de ces nouvelles finalités (conformément au Principe 1 de confidentialité des données) et confirmer que :
 - la **personne concernée** consent au **traitement** de ses **données à caractère personnel** pour cette nouvelle finalité ;
 - le **traitement** est requis en vertu d'une loi en vigueur ;
 - les nouvelles finalités du **traitement** des données à caractère personnel sont compatibles avec les finalités initiales du **traitement** ; ou
 - le **traitement** est légal en vertu des lois en vigueur sur la confidentialité des données.

Le **traitement** visant de nouvelles finalités ne sera déclaré compatible avec les finalités initiales que lorsque la loi en vigueur le permet, ou lorsqu'après évaluation de notre part, nous avons conclu qu'il tient compte de facteurs tels que la relation entre les finalités initiales et les nouvelles finalités ; le contexte dans lequel les **données à caractère personnel** ont été recueillies et les attentes des **personnes concernées** ; la nature des **données à caractère personnel** ; les conséquences du nouveau **traitement** pour les **personnes concernées** ; et l'existence ou non de mesures de protection de la vie privée.

- **Minimisation des données traitées** : Nous ne devons **traiter** que les **données à caractère personnel** requises en ce qui a trait à la finalité concernée, et uniquement dans la mesure nécessaire à cette finalité. Le **traitement des données à caractère personnel** que nous effectuons doit être précis et pertinent, et éviter tout excès.

Principe 3 de confidentialité des données : nous assurons le maintien de la qualité des données recueillies

Lorsque nous traitons des **données à caractère personnel**, nous prenons des mesures appropriées pour :

- confirmer que les **données à caractère personnel** sont exactes et mises à jour lorsque cela est nécessaire ; et
- dans le cas où des **données à caractère personnel** sont requises pour prendre des décisions relatives à une personne concernée mais qu'elles sont inexactes, ces **données à caractère personnel** sont supprimées, rectifiées ou complétées (en fonction de la finalité du traitement).

Principe 4 de confidentialité des données : nous sommes vigilants vis-à-vis les informations sensibles

Les **informations sensibles** constituent un type de **données à caractère personnel** de nature particulièrement privée, et comprennent notamment des données relatives aux origines raciales ou ethniques des personnes, à leur appartenance syndicale, à leur santé et à leurs données biométriques, ainsi qu'à leur casier judiciaire. Nous devons veiller à ce que le **traitement d'informations sensibles** ne se fasse qu'en cas de nécessité absolue et seulement si :

- la **personne concernée y consent** ; ou
- si le **traitement** est :
 - nécessaire au respect des obligations légales,
 - expressément autorisé par les lois locales sur la confidentialité des données personnelles ou les lois du travail locales et si les **données à caractère personnel** en question proviennent du pays concerné ; ou
 - nécessaire afin de prévenir ou d'atténuer une menace imminente grave pour la vie, la santé ou la sécurité d'une personne.

Principe 5 de confidentialité des données : nous protégeons la divulgation des données à caractère personnel

Nous protégeons la **divulgation** des **données à caractère personnel** (y compris, mais sans s'y limiter, lorsqu'elles sont transférées au-delà des frontières nationales) de la façon suivante ;

- **Divulgations hors du Groupe Rio Tinto** : Si nous devons divulguer des **données à caractère personnel** hors du **Groupe Rio Tinto** (par exemple, à un prestataire de services ou à une tierce partie qui est autorisée à recevoir ces **données à caractère personnel**), nous devons nous assurer :
 - que la **divulgation** est protégée par des clauses contractuelles sur la confidentialité des données, approuvées par le département Éthique & intégrité ou par les Services juridiques de Rio Tinto. Ceci doit notamment inclure une évaluation visant à définir si d'éventuels transferts au-delà des frontières nationales respectent les lois en vigueur sur la confidentialité des données (voir exigences à l'Annexe 2b) ;
 - que les **personnes concernées** ont **consenti** à la **divulgation** ; ou
 - que la **divulgation** est exigée par la loi ou expressément autorisée par les lois locales sur la confidentialité des données personnelles et que les **données à caractère personnel** concernées proviennent de ce territoire.
- **Divulgations au sein du Groupe Rio Tinto** : Les divulgations au sein du **Groupe Rio Tinto** sont protégées par l'**Acte de transfert de données de Rio Tinto** s'il est nécessaire de transmettre des **données à caractère personnel** à l'extérieur du pays où celles-ci ont été initialement collectées. Le Secrétariat d'entreprise et les **entités du Groupe** veilleront à ce que toute nouvelle société du Groupe signe l'**Acte de transfert de données de Rio Tinto**.

Un aperçu des divulgations/transferts internationaux (au sein du Groupe Rio Tinto et à des prestataires externes) est fourni à l'Annexe 2a.

Principe 6 de confidentialité des données : Nous devons sécuriser les données à caractère personnel

- **Obligations générales en matière de sécurisation des données** : Les **données à caractère personnel** doivent être conservées de façon sûre et protégées contre les **traitements** accidentels ou illicites, notamment contre la perte et l'accès non autorisé, la destruction, la mauvaise utilisation, la modification ou la **divulgation**. Cela signifie qu'il faut veiller à ce que Rio Tinto ait mis en place des mesures techniques et organisationnelles appropriées. Les obligations en matière de sécurité des données s'appliquent, que celles-ci soient conservées sous forme imprimée (sur papier) ou électronique (dans une base de données). Voici les principales règles à suivre :
 - l'accès aux **données à caractère personnel** autres que celles nous appartenant est réservé uniquement aux personnes qui ont besoin de les connaître ; et
 - les **entités du Groupe** doivent appliquer [Norme](#) de Rio Tinto sur l'utilisation acceptable de l'information et des ressources électroniques et la [Procédure du groupe](#) sur l'information et la **cybersécurité** (administrée par le service Cybersécurité du département S&TI) afin de garantir que les mesures adéquates de sécurité physique, technique et organisationnelle soient en place à chaque étape du « cycle de vie » des **données à caractère personnel**.
- **Signalement interne sur les incidents liés à la confidentialité des données personnelles** : Les **incidents liés à la confidentialité des données personnelles** doivent être immédiatement signalés au département Éthique et intégrité. Lorsque les lois en vigueur sur la confidentialité des données l'exigent, le département Éthique et Conformité s'assurera que toute **violation des données** est notifiée à(aux) autorité(s) compétente(s) et aux **personnes concernées**.

Principe 7 de confidentialité des données : nous limitons la sauvegarde des données personnelles

Les **données à caractère personnel** doivent être conservées pendant une durée qui n'excède pas la durée dictée par la finalité licite pour laquelle elles sont **traitées** (telle que notifiée aux personnes concernées), ou pendant la durée requise ou autorisée par les lois locales (selon la période la plus courte). Les **données à caractère personnel** seront conservées conformément au Calendrier de rétention et de destruction des dossiers (établi conformément à la Norme de gestion des dossiers et actualisé régulièrement), qui définit la durée pendant laquelle les différents types de dossiers contenant des données à caractère personnel doivent être conservés. Au-delà de cette durée, les dossiers contenant des **données à caractère personnel** doivent être détruits conformément aux exigences de sécurité (dans le cas des dossiers physiques) ou supprimés définitivement (dans le cas des dossiers électroniques), conformément au Calendrier Rio Tinto de rétention et de destruction des dossiers ou aux lois locales en vigueur (selon la réglementation imposant les obligations les plus strictes). Dans la mesure du possible, tous les exemplaires archivés et de sauvegarde doivent être détruits en même temps que chaque dossier original contenant les **données à caractère personnel**, et selon la même procédure.

Principe 8 de confidentialité des données : nous respectons les droits des personnes concernées

Les **personnes concernées** ont le droit :

- de demander l'accès aux **données à caractère personnel** que Rio Tinto conserve sur elles ;
- de demander la correction des **données à caractère personnel** qui sont inexactes, incomplètes ou obsolètes ;
- de demander la suppression de leurs **données à caractère personnel** ;
- de connaître la façon dont leurs **données à caractère personnel** sont **traitées** ;
- d'exiger la cessation du **traitement** de leurs **données à caractère personnel** (en particulier si le traitement est susceptible de causer un préjudice ou s'il sert à des fins de marketing direct) ;
- d'être avisées en cas de décision prise à leur sujet par les **entités du Groupe** basée uniquement sur le **traitement** automatisé de données (afin de pouvoir demander une révision de cette décision, au besoin) ;
- de déposer une plainte concernant le **traitement** de leurs **données à caractère personnel** ; ou
- de retirer le **consentement** donné précédemment pour le **traitement** de leurs **données à caractère personnel** par Rio Tinto.

Des exceptions juridiques peuvent s'opposer à l'exercice de ces droits, et Rio Tinto évaluera les demandes au cas par cas en se référant à la législation du pays où est située la **personne concernée** (ou, si le pays où est située la personne concernée ne dispose pas de lois sur la confidentialité des données, en se référant aux lois australiennes sur la confidentialité des données). Les demandes des **personnes concernées** visant à se prévaloir de leurs droits doivent être transmises au **responsable de la confidentialité des données personnelles** pour la région concernée, qui conseillera sur les modalités à suivre pour répondre aux demandes. Vous trouverez à l'annexe 3 de plus amples informations sur les modalités à suivre pour exercer les droits à la protection des données personnelles.

Principe 9 de confidentialité des données : Nous assurons le respect de la vie privée dès la conception

Nous devons veiller à ce que les mesures de confidentialité des données soient intégrées dans nos activités de traitement des données à caractère personnel.

Évaluation du seuil de confidentialité :

Le département Éthique & Conformité effectuera une évaluation du seuil de confidentialité s'il est proposé :

- d'introduire un nouveau système ou une nouvelle technologie de traitement des données personnelles ou une version étendue du système/de la technologie ;
- d'externaliser des fonctions de traitement des données à caractère personnel ; ou
- de recueillir ou de générer de nouvelles catégories de données à caractère personnel ou de traiter en vue de nouvelles finalités les données à caractère personnel existantes.

L'évaluation du seuil de confidentialité tiendra compte :

- de la nature des données à caractère personnel ;
- de la finalité proposée pour le traitement ;
- des divulgations proposées pour les données à caractère personnel, notamment tout flux de données transfrontalier proposé.

Ces informations seront recueillies dans le cadre du processus d'évaluation des risques de sécurité (**SRA**) effectué par le service Cybersécurité ou séparément par le département Éthique et Conformité.

Évaluation d'impact sur la vie privée :

Si l'Évaluation de seuil de confidentialité indique que le traitement proposé est susceptible d'entraîner un risque élevé pour les droits à la vie privée des personnes concernées, le département Éthique et Conformité effectuera une Évaluation d'impact sur la vie privée. L'Évaluation d'impact sur la vie privée identifiera les mesures à prendre pour réduire le risque et pour s'assurer que Rio Tinto respecte ses obligations en vertu de la présente Norme et des lois en vigueur sur la confidentialité des données.

Principe 10 de confidentialité des données : nous n'envoyons pas de pourriel

Nous devons limiter notre utilisation des **données à caractère personnel** en ce qui a trait à l'envoi de **communications de marketing**. Toutes les **communications de marketing** (peu importe leur mode de distribution) doivent :

- indiquer clairement le nom et les coordonnées de l'**entité** ou de la société du Groupe qui est à l'origine du message ;
- être envoyées avec le consentement du (de la) destinataire/**personne concernée**, à moins que le département Éthique et Conformité n'ait spécifié que le consentement n'est pas requis dans les pays où les destinataires proposés sont situés ; et
- contenir un mécanisme de désabonnement de la liste d'envoi ou de retrait du consentement. Les volontés exprimées au moyen de ce mécanisme doivent être mises en application, et les dossiers modifiés en conséquence.

Glossaire

Le **Consentement** d'une **personne concernée** désigne l'indication précise, informée et sans ambiguïté, donnée librement, des souhaits de la **personne concernée**.

Les **Informations relatives au casier judiciaire** désignent les **données à caractère personnel** relatives à des infractions pénales et condamnations.

La **Violation des données** désigne une violation de la sécurité entraînant la destruction, la perte, la modification, la **divulgation** ou l'accès non autorisé des/aux **données à caractère personnel** transmises, conservées ou **traitées**.

Un **Incident lié à la confidentialité des données** désigne une **violation des données** ou une violation connue ou suspectée de l'un des autres **principes de confidentialité des données** énoncés dans la présente Norme de confidentialité des données.

Un **Responsable de la confidentialité des données** désigne un membre du département Éthique et Conformité qui sert de premier point de contact pour toutes les questions de confidentialité des données personnelles relevant de votre région, tel qu'indiqué sur la page Confidentialité des données dans Element.

Les **Principes de confidentialité des données** désignent les principes énoncés dans la présente Norme de confidentialité des données que les sociétés et le personnel du Groupe Rio Tinto doivent appliquer pour le **traitement de données à caractère personnel**.

La **Personne concernée** désigne la personne à laquelle se rapportent les **données à caractère personnel**.

La **Divulgation** désigne l'action par laquelle les données à caractères personnel deviennent accessibles à autrui.

Les **Entités du groupe** désignent tou(te)s les sociétés, groupes de produits, unités d'affaires, fonctions générales et sièges sociaux du groupe Rio Tinto.

Une **Fin commerciale légitime** désigne une intention visant à ce que Rio Tinto atteigne ses propres objectifs commerciaux, en respectant l'ensemble des lois et règlements en vigueur ainsi que les politiques et normes de Rio Tinto.

Les **Communications de marketing** désignent les communications et publications visant à commercialiser ou à promouvoir Rio Tinto ou ses produits, exclusion faite des communications de Rio Tinto à son personnel en lien avec l'administration des relations employeur-employés.

Le terme **Données personnelles** désigne toute information liée à un individu que l'on peut identifier.

L'**Évaluation d'impact sur la vie privée** désigne l'évaluation de l'impact des opérations de **traitement** proposées sur les droits et libertés des **personnes concernées**, et la protection des **données à caractère personnel**.

La **Déclaration de confidentialité** désigne l'avis à fournir aux **personnes concernées** au moment où nous recueillons leurs **données à caractère personnel**.

Le **Traitement** désigne l'ensemble des opérations portant sur des **données à caractère personnel**, telles que la collecte, l'utilisation, la divulgation, l'enregistrement, l'organisation, le stockage, le transfert, la modification, la suppression, la destruction, la récupération, l'accès, l'hébergement ou toute autre manipulation.

L'**Acte de transfert de données de Rio Tinto** désigne l'acte conclu par Rio Tinto Limited et Rio Tinto plc le 1^{er} juillet 2009 (ou tel que modifié ultérieurement) et auquel sont liées les sociétés du groupe Rio Tinto en vertu de l'Acte d'adhésion qu'elles ont signé.

Le **Groupe Rio Tinto** désigne toutes les entités appartenant directement ou indirectement, en totalité ou en majorité, à Rio Tinto plc ou à Rio Tinto Limited, ou gérées par ces sociétés.

Les **Informations sensibles** désignent des **données à caractère personnel** (y compris renseignements ou opinions) relatives aux origines raciales ou ethniques d'une personne, à ses opinions et appartenances politiques, ses croyances religieuses ou philosophiques, ses associations, son appartenance syndicale, **son casier judiciaire**, ses données génétiques, ses données biométriques (**traitées** dans le but d'identifier uniquement une personne physique) ou qui sont relatives à sa santé, aux services de santé reçus ou à sa vie sexuelle.

Annexe 1

Aperçu de la collecte et du traitement des données à caractère personnel

Rio Tinto recueille et traite des **données à caractère personnel** pour des finalités commerciales, dont certaines sont présentées ci-dessous.

- Gestion des données personnelles : Des **données à caractère personnel** sur les employés et les prestataires de services sont obtenues à des fins de gestion par les RH. Ces données concernent l'identité, les coordonnées, les antécédents professionnels, la formation et les qualifications, le rendement, ainsi que les renseignements nécessaires au versement du salaire ou de la rémunération et à l'octroi d'autres avantages sociaux ;
- Gestion des relations d'affaires avec les clients, les fournisseurs et autres tiers (notamment des individus employés par des partenaires en coentreprise). Des **données à caractère personnel** sur des membres d'organisations externes sont recueillies à des fins commerciales, comme l'achat de biens ou l'acquisition de services, la conclusion et l'exécution de contrats et pour des besoins de communications. Ces données se limitent généralement aux coordonnées ;
- Gestion des relations avec les actionnaires : Des **données à caractère personnel** sont obtenues auprès des actionnaires de Rio Tinto à des fins liées à leur actionnariat, y compris l'émission ou la négociation d'actions, le versement de dividendes, la présentation de l'information exigée par la réglementation et les communications. Ces **données à caractère personnel** peuvent inclure le nom, l'adresse, les actions détenues, le numéro de dossier fiscal et les détails du compte bancaire de l'actionnaire.
Les **données à caractère personnel** des actionnaires sont recueillies par Rio Tinto ou en son nom, par le gestionnaire externe de notre registre des actionnaires. Occasionnellement, ces données peuvent être transmises à d'autres prestataires de services pour le paiement des dividendes ou l'envoi de communications aux actionnaires ou, dans la mesure où la loi le permet, aux courtiers en valeurs autorisés, aux inspecteurs du registre, aux acheteurs potentiels de titres de Rio Tinto ou à certains organismes de réglementation, dont l'Australian Taxation Office ;
- Sûreté, sécurité et obligations légales : Des **données à caractère personnel** sont recueillies sur les visiteurs de nos sites pour des raisons de sûreté et de sécurité. Il peut s'agir d'images de télévision en circuit fermé, lorsque les lois locales l'autorisent. Rio Tinto recueille aussi des **données à caractère personnel** dans l'exercice de ses obligations légales (par exemple, pour satisfaire aux exigences de la législation contre le blanchiment d'argent et des lois en matière d'alerte professionnelle) ;
- Gestion des relations avec les communautés : Des **données à caractère personnel** sont obtenues des membres des communautés où Rio Tinto exerce des activités d'exploitation minière et autres, dans le but d'échanger et d'interagir avec ces communautés.

Dans la mesure du possible, Rio Tinto recueille les **données à caractère personnel** directement auprès des **personnes concernées**.

Les **données à caractère personnel** peuvent être stockées dans les bases de données ou les systèmes locaux de Rio Tinto, dans la Solution d'affaires de Rio Tinto (système SAP hébergé en Australie) ou sur une infrastructure détenue et exploitée par des prestataires de services engagés par Rio Tinto. Lorsque des prestataires de services ont le mandat d'aider Rio Tinto à **traiter des données à caractère personnel**, Rio Tinto exige d'eux qu'ils se conforment aux obligations de protection et de confidentialité des données que leur impose leur contrat, ainsi qu'aux lois en vigueur sur la confidentialité des données.

Annexe 2

Divulgations internationales

a. Aperçu des Divulgations internationales

Le [site internet de Rio](#) présente un aperçu des activités mondiales du groupe Rio Tinto et des pays où il exerce ses activités. Il explique en outre les opérations de chacun des groupes de produits de Rio Tinto, par pays.

Si vous êtes employé ou embauché par un groupe de produits particulier de Rio Tinto ou que vous entretenez des relations d'affaires avec lui, les sociétés du groupe Rio Tinto établies dans les pays énumérés pour ce groupe de produits peuvent échanger vos **données à caractère personnel**.

De plus, vos **données à caractère personnel** peuvent être **traitées** par les sociétés de Rio Tinto qui fournissent des « services partagés » ainsi que par les prestataires de services qui offrent leurs services au groupe Rio Tinto dans un ou plusieurs des pays suivants :

- **sociétés de Rio Tinto qui fournissent des « services partagés »** : Afrique du Sud, Australie, Canada, États-Unis, Inde, Mongolie, Royaume-Uni, Singapour.
- **prestataires de services** qui aident le groupe Rio Tinto à exercer les fonctions de RH à l'échelle mondiale et d'autres fonctions de services partagés, et qui traitent des **données à caractère personnel** au nom d'une ou de plusieurs sociétés du groupe Rio Tinto situées dans les pays suivants : Australie, Canada, Union Européenne, Inde, Malaisie, Philippines, Pologne, Royaume-Uni et États-Unis.

Les **données à caractère personnel** des actionnaires sont traitées en Australie et au Royaume-Uni par Rio Tinto et par le gestionnaire externe de notre registre des actionnaires.

b. Évaluation préalable aux divulgations internationales

Préalablement au transfert de **données à caractère personnel** hors du pays où elles ont été recueillies, les entités concernées du Groupe effectueront l'évaluation suivante (avec l'assistance du département Éthique & Conformité) :

- Nous vérifierons que les **personnes concernées** ont bien été informées que leurs **données à caractère personnel** allaient être transférées.
- Nous vérifierons si le transfert est couvert par des dispositions de transfert ultérieures ou d'autres dispositions précisées dans l'accord interentreprises de Rio Tinto (Acte de transfert de données de Rio Tinto) ou si des clauses additionnelles sont nécessaires.
- Les transferts internationaux d'**informations sensibles** exigent une évaluation du département Éthique et Conformité.
- Pour les **divulgations** hors du Groupe Rio Tinto, nous nous assurerons que la tierce partie est en mesure d'assurer la sécurité et la confidentialité des **données à caractère personnel**. Nous pourrions demander à la tierce partie de fournir une description des mesures techniques et organisationnelles mises en place pour protéger les **données à caractère personnel**. L'équipe chargée de la cybersécurité de Rio Tinto évaluera si ces mesures sont suffisantes (par ex. dans le cadre de son Évaluation des risques de sécurité).

Annexe 3

Droits et plaintes des personnes concernées

a. Droits généraux de la personne concernée

Veuillez remplir un **formulaire de demande de la personne concernée** si vous désirez exercer votre droit en application du Principe 8 de confidentialité des données, notamment :

- de demander l'accès à vos **données à caractère personnel** conservées par Rio Tinto ;
- de demander la correction des **données à caractère personnel** qui sont inexactes, incomplètes ou obsolètes ;
- de savoir comment vos **données à caractère personnel** sont traitées ; ou
- selon que le droit à la « portabilité des données » est un droit en vertu des lois de votre pays sur la confidentialité des données, de recevoir un exemplaire de vos **données à caractère personnel** sous un format structuré, couramment utilisé et lisible par machine, et demander que nous transmettions à une tierce partie les données à caractère personnel que vous nous fournissez ;
- selon que le droit à exiger la cessation du traitement est un droit en vertu des lois de votre pays sur la confidentialité des données, d'exiger la cessation temporaire ou permanente du traitement de vos **données à caractère personnel** (par exemple, si l'exactitude de **ces données** est contestée ou si vous considérez que le **traitement** est illégal, ou s'il est susceptible de causer un préjudice ou s'il sert à des fins de marketing direct) ; ou
- de demander des informations concernant les méthodes utilisées pour transférer vos **données à caractère personnel**, ou un exemplaire de ces méthodes ;
- de retirer le **consentement** que vous avez donné précédemment pour le **traitement** par Rio Tinto de vos **données à caractère personnel**.

Votre demande sera transmise au **Responsable de la confidentialité des données** de votre région, qui pourra aussi vous fournir le *Formulaire de demande de la personne concernée*. Rio Tinto tentera d'accéder à votre demande dans un délai raisonnable après la transmission de la demande ou après la réception de l'information nécessaire pour la **traiter** (ou selon les autres exigences des lois locales).

b. Questions ou plaintes

Si vous avez des questions à poser ou si vous souhaitez déposer une plainte à propos du **traitement** de vos **données à caractère personnel**, vous pouvez le faire en écrivant à l'adresse aske&C@riotinto.com ou en le signalant au département Éthique et intégrité sous la forme d'un **Incident lié à la confidentialité des données personnelles**.

Les **Responsables de la confidentialité des données** sont chargés de mener une enquête sur les plaintes et d'y répondre, sauf si leur **traitement des données à caractère personnel** est en cause. Dans ce cas, une autre personne sera désignée pour enquêter et répondre à la plainte. Si vous n'êtes pas satisfait de la réponse à votre plainte, vous pouvez le signaler, lorsqu'ils existent, à l'organe de réglementation de la confidentialité des données ou à l'autorité de protection des données de votre pays.