General

Owner: Global General Counsel I Author: Global General Counsel I Approved: 15.12.2023 I Version: 1.0 I Classification: Public

Data Protection Compliance at Control Risks

In this addendum, "**consent**", "**entrusted party**", "**individual**", "**personal information**", "**personal information handler** or **PI handler**", "**processing** or **handling**", and "**sensitive personal information**" mean those concepts, roles and activities as defined in the Personal Information Protection Law of China (the "**PIPL**") or any implementing regulations issued by the Chinese Government, including the Cyberspace Administration of China (the "**CAC**").

This China Addendum supplements our Data Protection Narrative (the "**Data Protection Narrative**") here:https://www.controlrisks.com/-/media/corporate/files/legal/trust-centre/data-protection-narrative.pdf and provides information to our clients about our compliance with PIPL where the requirements differ. Where there is a conflict between the Data Protection Narrative and this China Addendum, the terms of this China Addendum shall apply solely with regards to our activities in mainland China

For more information on how we process personal information in China, please see our Privacy Policy (China Addendum) here.

1. COMPLIANCE REQUIREMENTS

Lawful basis for processing

Where we are the PI handler for personal information, we have established the lawful basis for all personal information processing activities, and they have been documented as part of our processing records.

We may process personal information on the following grounds under PIPL:

- with the consent of the individual;
- where it is necessary for the conclusion or performance of a contract to which the individual is a party;
- where it is necessary for the performance of statutory duties or statutory obligations;
- where it is necessary for coping with public health emergencies or for the protection of the life, health, and property of a natural person;

- where such acts as news reporting and supervision by public opinions are carried out for the public interest, and the processing of personal information is within a reasonable scope;

- where the personal information disclosed by individuals themselves or other legally disclosed personal information is processed within a reasonable scope; or

- other circumstances provided by laws and administrative regulations.

Where clients are PI handlers in their own right, they will be required to have their own lawful basis for processing.

2. KEY SERVICES

2.1. Business intelligence ("BI"), investigations and political and economic risk consulting (Control Risks acts as an entrusted party)

Personal information is collected through open-source research, which includes public record (such as press articles, corporate filings, court records, and the records of central and local government departments and statutory bodies), news aggregators, specialist databases, social media and deep-web research, and source enquiries with suitable individuals. It is also received directly from the client or its advisers or from investigative interviews with potential suspects, witnesses or other individuals. When assisting with investigations, personal information may also be collected using forensic imaging, data collection and eDiscovery services (see section 2.3 of this addendum).

The categories of personal information which are processed are those reasonably required to fulfil the client's enquiry, such as the individual's name, age, gender, employment status, address/location, nationality, marital status, contact details (such as telephone and email address), education, professional career, expressions of opinion about an individual's business integrity, and business connections and affiliations. Depending on the specific circumstances we may also process sensitive personal information, including political opinion.

Control Risks acts under the instructions of the client to provide BI, investigations and political and economic risk consulting services and will be an entrusted party for the client.

In relation to databases which Control Risks interrogates or enables the client to interrogate, the database owner will typically be a PI handler for personal information contained in its database. Although Control Risks will be an entrusted party in relation to its processing of personal information in the database on behalf of the client, the database owner will therefore be a PI handler rather than an entrusted party on behalf of Control Risks.

For our data flow diagrams for BI, investigations and political and economic risk consulting services, please see the Data Protection Narrative.

2.2. VANTAGE Diligence, Platform, Screening and Compliance Solutions (Control Risks acts as an entrusted party)

VANTAGE Diligence

Personal information is collected through open-source research, which includes public record (such as press articles, corporate filings, court records, and the records of central and local government departments and statutory bodies), news aggregators, specialist databases, social media and deep-web research, and source enquiries with suitable individuals. It is also received directly from the client or its advisers sometimes via a partner service website, for example where the GAN platform is used.

Control Risks acts under the instructions of the client to provide Vantage Diligence services and will be an entrusted party for the client.

For our data flow diagrams for VANTAGE Diligence services, please see the Data Protection Narrative.

VANTAGE Platform

For more information about our processing activities for these services, please see the Data Protection Narrative. .

VANTAGE Screening

For more information about our processing activities for these services, please see the Data Protection Narrative.

VANTAGE Compliance Solutions

For more information about our processing activities for these services, please see the Data Protection Narrative.

2.3. Forensic imaging, data collection and eDiscovery services (data filtering, processing, analytics, hosting, production and project management) (Control Risks acts as an entrusted party)

For more information about our processing activities for these services, please see the Data Protection Narrative.

2.4. Security risk consultancy including security design engineering, security risk assessments, outsourced security services and crisis management (the "Control Risks Security Consulting Services") (Control Risks acts as PI handler)

For more information about our processing activities for these services, please see the Data Protection Narrative.

2.5. Protective services, High Risk Managed Services and journey management (Control Risks acts as an entrusted party)

For more information about our processing activities for these services, please see the Data Protection Narrative

2.6. Cyber Threat Intelligence, Protect and Response Services (Control Risks as an entrusted party)

Personal information is collected through open-source research, which includes public record (such as press articles, corporate filings, court records, and the records of central and local government departments and statutory bodies), news aggregators, specialist databases, social media and deep-web research, and source enquiries with suitable individuals. It is also received directly from the client or its advisers - or by accessing information hosted on the client's systems - or from investigative interviews with potential suspects, witnesses or other individuals. Personal information may also be collected using forensic imaging, data collection and eDiscovery services (see section 2.3 of this document).

The categories of personal information which are processed are those reasonably required to fulfil the client's enquiry, such as the individual's name, age, gender, employment status, address/location, nationality, marital status, contact details (such as telephone and email address), education, and professional career and expressions of opinion. Depending on the specific circumstances we may also process sensitive personal information, including, trade union membership and political opinion and financial data.

We process personal information under client instruction as an entrusted party for these services.

For our data flow diagrams for Cyber Threat Intelligence, Protect and Response services, please see the Data Protection Narrative.

2.7. Response Services other than Cyber Response Services (Control Risks acts as PI handler)

For more information about our processing activities for these services, please see the Data Protection Narrative.

2.8. Seerist and Seerist CORE ("Seerist") (Control Risks, including its subsidiary Seerist, acts as an entrusted party)

For more information about our processing activities for these services, please see the Data Protection Narrative.

2.9. Control Risks ONE (Control Risks acts as a PI handler or entrusted party)

For more information about our processing activities for these services, please see the Data Protection Narrative.