Control Risks GDPR Compliance

In this document, “consent”, “controller”, “data protection impact assessment”, “data subject”, “personal data”, “processing”, “processor” and “special categories of personal data” mean those concepts, roles and activities as defined in the GDPR.

1. COMPLIANCE REQUIREMENTS

1.1. Data protection officer (“DPO”)

- DPO (Group): Sally McNairScott email: legal@controlrisks.com
- DPO (Germany): Peter Christian Felst email: Peter.Felst@Mazars.DE

1.2. Controller- processor responsibilities

When processing personal data in the context of providing our services, we regard ourselves as controller where we make decisions on how personal data is used in connection with our services, and processor where we only use personal data as allowed by our clients. Where we are processor, we provide a standard data processing agreement (“DPA”) as an appendix to our contract with clients in accordance with article 28 of the GDPR.

1.3. Data processing records

We maintain controller records of data processing activities including information security and data protection impact assessments, the lawful basis for processing and data flow diagrams, in each case where required. We also maintain processor records of data processing activities.

1.4. Conditions for lawful basis for processing

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

The lawful basis for processing personal data under the GDPR article 6 and where applicable article 9 will be one or more of the following, depending on the nature of the data and the project:

- with the consent of the data subject;
necessary for entering into, or performing, a contract;

necessary for the purpose of Control Risks’ or our client’s legitimate interests;

necessary to protect the vital interests of a data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

necessary for the prevention or detection of an unlawful act;

necessary for the establishment, exercise or defence of a legal claim;

necessary for compliance with a legal obligation; and

the data has been manifestly made public by the data subject.

Where clients are controllers in their own right and they are subject to the GDPR, they will be required to have their own lawful basis for processing.

1.5. Privacy policy and notice

As a controller we provide privacy notices to data subjects unless to do so would prove impossible or would involve a disproportionate effort or otherwise would render impossible or seriously impair the achievement of the objectives of the processing. We provide a public Privacy Notice on our website to explain why and when we, as a controller, collect personal data as well as providing other information to data subjects about our processing of their personal data, who we may share their personal data with and their data subject rights. We may act as a controller in relation to certain services (as described in more detail below) and we may also act as controller for personal data processing which is unconnected with the services we provide. For example, in relation to our client or prospective client contacts who we may wish to contact occasionally about products and services that could be of interest to them and also information gathered about our website users such as browsing habits.

We have a group Data Protection Policy to ensure our employees comply with applicable data protection laws. Our group Data Protection Policy forms part of the induction programme for all new staff so that all employees are aware of the GDPR and data protection restrictions and obligations generally. Refresher training is provided every two years for data protection and annually for information security.

1.6. Data subject rights

We have implemented response procedures for data subject access requests which allow data subjects to exercise their rights to access, rectify and delete their personal data in accordance with the GDPR where we are a controller for their data. Data subject correction, deletion and portability requests are infrequent. Should Control Risks receive such requests, they would be forwarded to its DPO, responded to promptly and adequately and data subjects would be able to (i) determine whether their personal data is correct, (ii) have their personal data deleted in accordance with their legal rights, and/or (iii) have their personal data transferred to another entity if applicable criteria are met.

Where we act as processor of personal data on behalf of a client, if a request is received directly from a data subject we will contact the controller client for instructions on dealing with the request.

1.7. Privacy and data protection impact assessments

Where we, as controller, process personal data that is considered high risk, or when we process such information in a new way requiring new tools, assessments are carried out to comply with article 35 requirements of the GDPR. These assessments allow us to implement appropriate technical and organisational measures and integrate the necessary safeguards into the processing in order to meet the requirements of this regulation and protect the rights of data subjects. As a processor we will, on request, assist our controller clients with their own data protection impact assessments relating to the services we provide to them.
1.8. Breach management
Under our procedures for incident management, we ensure that we have safeguards and measures in place to detect, assess, investigate and report any personal data breach at the earliest possible time. All employees have been made aware of the reporting lines and steps to follow if confidential information is lost or compromised or suspected of being lost or compromised. Governance is in place to ensure that following an incident appropriate root cause analysis is conducted and remediation plans are developed to address any risks identified and prevent recurrence. Where we are a processor for personal data, we will notify controller clients without undue delay of any personal data breach relating to personal data we process for them.

1.9. Location of information and data transfers
Control Risks International Limited, our parent company, is located in Jersey and the affiliated entities within the Control Risks group of companies are located throughout the world. During the provision of services, personal data may be transferred outside of a client's home country and may be stored in and accessed from multiple countries. We have put recognised procedures in place to secure, encrypt and maintain the integrity of any personal data that is transferred to countries outside the European Economic Area (“EEA”). If the country does not have adequacy status, we rely on the European Commission’s Standard Contractual Clauses, including for transfers of personal data to the US. In addition, our US entity, Control Risks Group LLC, continues to maintain Privacy Shield certification although we recognise that Privacy Shield participants can no longer rely on the Privacy Shield as a valid data protection mechanism to transfer data from the EU to the US.

1.10. Sub-Processors
Where we are a processor, we sometimes use sub-processors to process personal data for the purposes of providing services. We have set out details of those sub-processors and the location of the processing (List of sub-processors), in compliance with article 28 of the GDPR.

1.11. Special categories of personal data
We process limited special category personal data and only in exceptional cases. We collect as much information as is required for the purpose of providing services and where we are a controller for the special category personal data, always in accordance with article 9 of the GDPR.

1.12. Information security and accountability
We have an Information Security Management System that runs from head office audited and certified to ISO 27001 by British Standards Institute. Our security measures which safeguard the confidentiality, integrity and availability of information include group policies; screening and training of Control Risks’ people; defined and audited processes; and technological controls such as, encrypted hard drives, segmented data stores, encrypted data backups, firewalls, network and communication security, two-factor authentication, and continuous monitoring. Only authorised personnel in Control Risks have access to the personal data. In addition, we have an internal auditor who checks adherence to company policies, to meet or exceed international standards.

Our third party service providers are expected, to the extent applicable, to provide the equivalent technical and organisational controls as the Control Risks group to protect the security and confidentiality of personal data and to commit to appropriate contract terms to ensure compliance with applicable data protection law.

1.13. Data retention and deletion
We have a group Data Retention, Archiving and Destruction Policy which sets out retention periods for storing information. Where we are the controller, personal data is retained for no longer than the minimum time needed, as required by applicable laws and regulations, or for the purposes for which it was collected. At the end of the defined period, personal data is permanently destroyed. Where we act as processor, clients may provide us with instructions to save data for or destroy or return data within, a specific period.
2. KEY SERVICES

2.1. Business intelligence (“BI”), investigations and political and economic risk consulting (Control Risks acts as processor other than for source data where Control Risks acts as controller)

Personal data 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 data may also be collected using forensic imaging, data collection and eDiscovery services (see paragraph 2.3).

The categories of personal data which are processed are those reasonably required to fulfil the client’s enquiry, such as the data subject’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 a data subject’s business integrity, business connections and affiliations and on occasion criminal record information. Depending on the specific circumstances we may also process special category personal data, 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 a processor for the client. The exception to this is in relation to personal data gathered from individuals who are sources for Control Risks. The identity of these sources and use of information which they provide is confidential to and controlled by Control Risks and Control Risks will be a controller for this personal data. Notwithstanding the foregoing, the client is the controller in relation to all information included in client deliverables, which respond to a client’s query.

In relation to databases which Control Risks interrogates or enables the client to interrogate, the database owner will typically be a controller in its own right for personal data contained in its database. Although Control Risks will be a processor in relation to its processing of personal data in the database on behalf of the client, the database owner will therefore be a controller in its own right rather than a sub-processor to Control Risks.
2.2. VANTAGE Diligence, Platform and Screening

VANTAGE Diligence (Control Risks acts as processor other than for source data where Control Risks acts as controller)

Personal data 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.

As with BI services referred to above, Control Risks acts under the instructions of the client to provide Vantage Diligence services and will be a processor for the client. The exception to this is in relation to personal data gathered from individuals who are sources for Control Risks. The identity of these sources and use of information which they provide is confidential to and controlled by Control Risks and Control Risks will be a controller for this personal data.

Notwithstanding the foregoing, the client is the controller in relation to all information included in client deliverables, which respond to a client’s query.

VANTAGE Platform (Control Risks acts as processor)

The platform is provided by our business partner, GAN Integrity, a specialist compliance software company based in New York (GAN Integrity, Inc.) and Copenhagen (GAN Integrity Solutions ApS).

Control Risks acts as a processor to the client in relation to Vantage Platform services. GAN is a sub-processor to Control Risks and GAN enters into DPAs with each of its own sub-processors in accordance with article 28 of the GDPR.
VANTAGE Screening (Control Risks acts as processor)

Personal data is collected using some of the industry’s largest risk intelligence databases (“External Content and Data Sources”):

- Dun & Bradstreet, Inc. (“D&B”): with offices at 103 John F Kennedy Parkway, Short Hills, NJ 07078.
- Lexis Nexis Risk Solutions FL Inc. (“Lexis Nexis”): a Minnesota corporation with offices at 1000 Alderman Drive, Alpharetta, Georgia 30005.

Control Risks will be a processor in relation to its processing of personal data in the D&B and Lexis Nexis databases on behalf of the client and D&B and Lexis Nexis will be sub-processors. D&B and Lexis Nexis will be controllers in their own right for personal data in their own databases and, where relevant, also in relation to the data received from clients that is used to set up and maintain the clients’ account and so will not be sub-processors to Control Risks in respect of this personal data.

GDPR Data Flow Diagram – 2.2 – Vantage Diligence, Platform and Screening

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

Personal data may be collected from personal computers, servers, mobile devices, structured database systems, source code systems, the cloud, social media and other digital sources.

Control Risks acts as processor for the client when providing forensic imaging, data collection and e-discovery services.
2.4. Security risk consultancy including security design engineering, security risk assessments, outsourced security services and crisis management (Control Risks acts as controller)

Personal data is collected direct from the client (or its advisers) when it contacts one of Control Risks’ offices, typically via telephone or email. We collect no more data than is required to fulfill the client’s request for assistance. Personal data is generally limited to contact details (such as name, job title, email address and work phone number). As this data may be retained in Control Risks’ databases for the purpose of contacting clients including about products and services we believe may be of interest to the client, Control Risks will be a controller for this contact data. We do not process any personal data as processor to provide these services to the client.
2.5. Protective services and journey management (Control Risks acts as processor)

Personal data is collected when the client (or its advisers) contacts one of Control Risks’ offices typically via telephone or email. We collect no more data than is required to fulfil the client’s request for assistance. This may include contact details of individuals to whom we provide the services (such as name, job title, email address, work phone number), passport details, blood type and other key medical data (in case of an emergency). In exceptional circumstances, we may also process special category data, such as biometric data and physical or mental health details.

For journey management and protective services, Control Risks typically acts as a processor for its client for the purpose of preserving life and safety of individuals.

We would only process special category personal data in circumstances where: (i) the data subject has provided explicit consent; or (ii) the processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent.
2.6. Cyber Threat Intelligence, Protect and Response Services (Control Risks as a processor rather than for source data where Control Risks acts as controller)

Personal data 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 data may also be collected using forensic imaging, data collection and eDiscovery services (see paragraph 2.3).

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

We process personal data under client instruction and categorise ourselves as a processor for these services. The exception to this is in relation to personal data gathered from individuals who are sources for Control Risks. The identity of these sources and use of information which they provide is confidential to and controlled by Control Risks and Control Risks will be a controller for this personal data. Notwithstanding the foregoing, the client is the controller in relation to all information included in client deliverables, which respond to a client’s query.
2.7. Response Services other than Cyber Response Services (Control Risks acts as controller)

These services are sometimes provided in support of an insurance policy taken-out with Hiscox Plc or another insurance company.

Personal data is collected about the data subject by one or more of the following methods: when the client, data subject or the data subject’s relatives or associates contact one of Control Risks’ offices (or an International SOS Assistance Centre) for assistance via telephone or email; directly from the insurance company; from 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.

The categories of personal data which are processed are those reasonably required to fulfil the client’s request for assistance, such as the data subject’s name, age, gender, employment status, address/location, nationality, marital status, contact details (such as telephone and email address), policy reference number and documents.

Depending on the specific circumstances in which our assistance is needed, we may also process special category personal data, including medical information, racial, ethnic, sexual orientation, religious beliefs, trade union membership, genetic and biometric data, political opinions and physical or mental health details.

We would only process special category personal data in circumstances where: (i) the data subject has provided explicit consent; or (ii) the processing is necessary to protect the vital interests of the data subject or of another natural personal where the data subject is physically or legally incapable of giving consent.
For Response Services, Control Risks, acts as a controller as Control Risks needs to make independent decisions about individuals and their data and act on its own initiative for the purpose of preserving life and safety of individuals.

2.8. CORE (Control Risks acts as controller)

Personal data is collected direct from a data subject - who is typically part of the client’s personnel - when they create their own profile and account for the purpose of accessing CORE content through the website. Personal data is limited and may include personal details such as name, location, job function, job seniority and contact details (such as telephone and email address). We may also process other personal data which a data subject includes in an inquiry. In creating the user’s profile, the data subject is made aware of our privacy policy, their rights are summarised and their consent must be given to any marketing.

In relation to contact information referred to above which is collected in connection with creation of profiles and accounts, Control Risks acts as controller. Control Risks also collects personal data from its websites for its own uses such as service improvement, data analytics and to use for marketing purposes. In relation to Control Risks’ collection of personal data for these purposes, Control Risks is also a controller.
2.9. eLearning (Control Risks acts as processor)

Personal data is collected direct from a data subject who is typically part of the client’s personnel - when they create their own profile and account for the purpose of accessing eLearning modules through the eLearning management system ("LMS"). Personal data is limited and may include personal details such as name, location, job function, job seniority and contact details (such as telephone and email address). We may also process other personal data which a data subject includes in an inquiry.

In relation to personal data processed to provide eLearning services to its clients Control Risks acts as processor for the client.

The LMS is provided by MINTRA Group, a sub-processor with whom we have a written agreement including a DPA and Standard Contractual Clauses in accordance with article 28 of the GDPR.
This diagram shows data flow scenarios for typical e-learning engagements.

Legend:
1) Details provided by the client, its advisors or other representatives.
2) The Control Risks website/same as the client engaging frame where information on services can be requested.
3) Information exchange can be seen a variety of mediums to suit the client, typically using the website, email or telephone.
4) Hard copy documents/media stored in on-site secure storage local to the office undertaking the work.
5) Where required, hard copy documents might be archived to a centralised secure document storage location.
6) Document/report location is either a Control Risks file server dedicated to the office undertaking the work or a Control Risks SharePoint Online/Teams/OneDrive instance geolocated to the office undertaking the work, where this is available.
7) Document/report backup location is housed either in Microsoft Azure or Amazon Web Services depending on office location.