General

Owner: Global General Counsel I Author: Global General Counsel I Approved: 15.12.2023 I Version: 4.1 I Classification: Public

Data Protection Compliance at Control Risks

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 applicable data protection laws. Where applicable data protection laws do not explicitly implement a term, the term shall be interpreted in accordance with the closest equivalent concept.

As a global organisation operating in many diverse jurisdictions, we have opted to apply the data protection principles of Regulation (EU) 2016/679 on the protection of personal data (the "**General Data Protection Regulation**" or the "**GDPR**"), including the GDPR as incorporated into UK legislation ("**UK GDPR**"), across our organisation, but particularly where applicable law has a lower standard of data protection. Nevertheless, Control Risks ensures compliance with specific processing and transfer requirements under applicable laws.

Our roles and activities under the Personal Information Protection Law of China (the "**PIPL**") may be different to those under the GDPR. For more information about Control Risks compliance with the PIPL and our key services in China please click here.

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
- DPO (Singapore): Adelene Seah email: legal@controlrisks.com

1.2. Controller- processor responsibilities

In jurisdictions with a distinction between "controller" and "processor", 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. Our standard DPA sets out the roles and responsibilities of the parties to the contract in accordance with applicable laws.

As a controller we ensure compliance with our obligations under all applicable laws as further described below.

1.3. Data processing records

We maintain 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. These may be provisioned to competent regulatory authorities upon request.

1.4. 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.

We may process personal data on the following grounds (where such basis exists under applicable law):

- with the consent of the data subject;
- as necessary for entering into, or performing, a contract;
- as necessary for the purpose of Control Risks' or our client's legitimate interests;
- as 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;
- as necessary for the prevention or detection of an unlawful act;
- as necessary for the establishment, exercise or defence of a legal claim;
- as necessary for compliance with a legal obligation; or
- the data has been manifestly made public by the data subject.

Where clients are controllers in their own right, 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 other 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 ("DSARs") which allow data subjects to exercise their rights to access, rectify and delete their personal data in accordance with applicable laws.
Our Privacy Policy (see section 1.5 of this document) directs data subjects to a dedicated email address to which they can submit their DSAR, 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.

1.7. 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 applicable laws. 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 applicable laws 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 throughout our group and may be stored in and accessed from multiple countries. Where necessary to ensure the purposes of the processing can be fulfilled, personal data may also be transferred to third party sub-processors (see below). We have put recognised procedures in place to secure, encrypt and maintain the integrity of any personal data that is subject to a cross-border transfer. If the transfer is considered "restricted" (i.e., the laws of the jurisdiction of the data importer are not considered to provide adequate protection of personal data by the legal standards of the jurisdiction of the data exporter), we ensure that appropriate legal measures are in place so that the transfer can proceed in accordance with applicable laws; this includes the implementation of standard contractual clauses ("**SCCs**") issued by a competent regulator, where applicable.

1.10. Transfer Impact Assessments

Restricted transfers from the United Kingdom or the European Economic Area (or that involve personal data governed by the GDPR or the UK GDPR) are subject to transfer impact assessments ("**TIAs**") following the European Court of Justice ruling in Data Protection Commissioner v. Facebook Ireland Limited, Maximillian Schrems (C-311/18) ("**Schrems II**"). In accordance with the Schrems II ruling and the subsequent guidance from the European Data Protection Board and Information Commissioner's Office, we conduct TIAs which evaluate:

- the specificities of the transfer;
- the surveillance laws of the data importer's country;
- the data protection laws of the data importer's country; and
- the options for data subjects to enforce their rights in the data importer's country.

Following the results of the assessment, we may implement mitigation measures to ensure personal data is protected to an adequate degree.

Summaries of TIAs we have conducted are available to clients upon request.

1.11. 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).

1.12. 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 applicable laws.

1.13. Information security and accountability

We have an Information Security Management System maintained and administered from our head office which is audited and certified to the ISO 27001 standard by the BSI. Our security measures which safeguard the confidentiality, integrity and availability of information include:

- group policies;
- screening and training of Control Risks' employees;
- 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 implement technical and organisational controls which are materially equivalent to those in place within 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.

1.14. 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 destroy or return data within a specific period.

2. KEY SERVICES

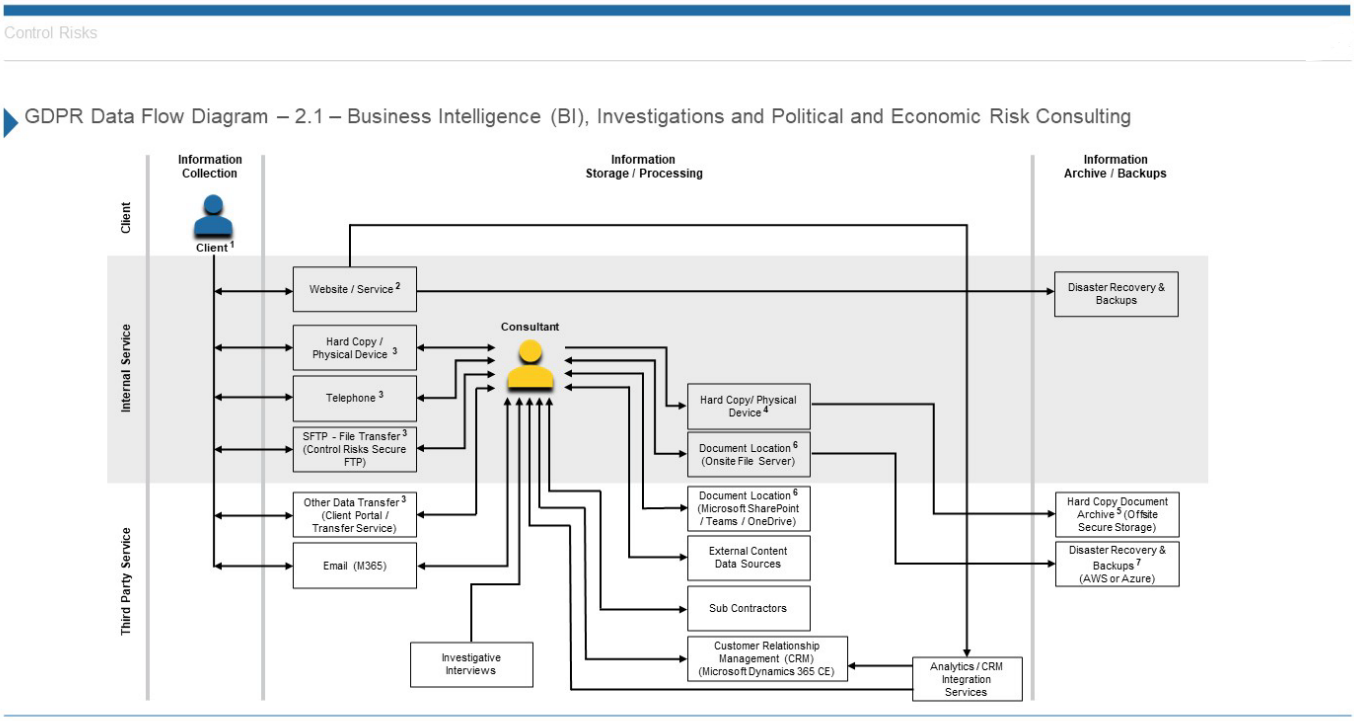
2.1. Business intelligence ("BI"), investigations and political and economic risk consulting (Control Risks acts as processor other than for source data where Control Risks acts as controller)

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 section 2.3 of this document).

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 or sent to 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 distinct controller 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 distinct controller rather than a sub-processor to Control Risks.



2.2. VANTAGE Diligence, Platform, Screening and Compliance Solutions

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 Control Risks' platform or 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 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 sometimes 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). The platform may also be provided by Control Risks.

Control Risks acts as an entrusted party to the client in relation to Vantage Platform services. Where the GAN platform is used, GAN is a sub-contractor to Control Risks and GAN enters into DPAs with each of its own sub-contractors in accordance with applicable law.

VANTAGE Automated 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.

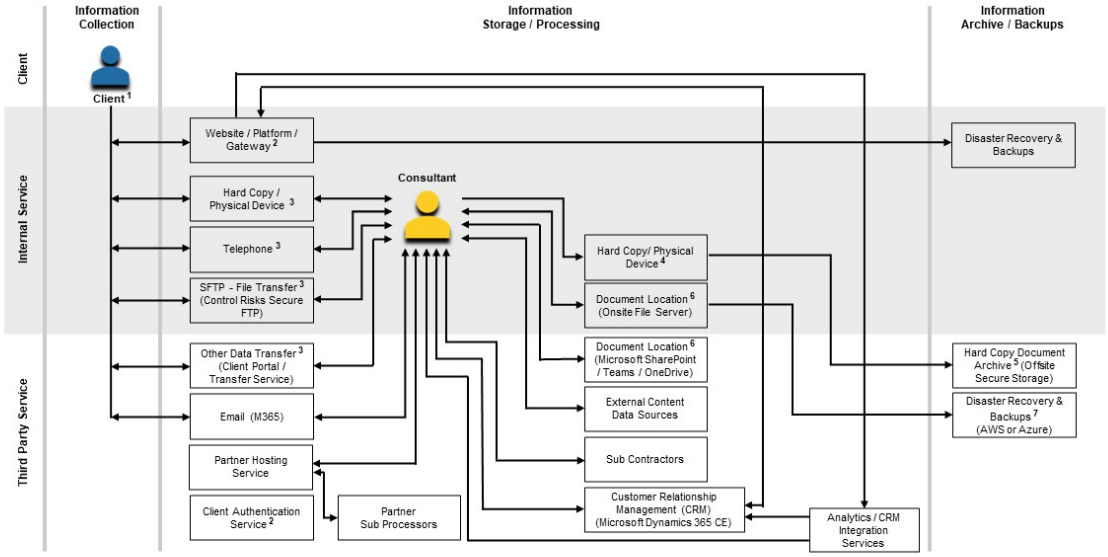
VANTAGE Compliance Solutions (Control Risks acts as processor)

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 (including due diligence questionnaires) with individuals or third parties.

The categories of personal data which are processed are those reasonably required to fulfil the client's compliance requirements, 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.

Control Risks acts in accordance with the client's instructions to provide VANTAGE Compliance Solutions and will be processor for the client.

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

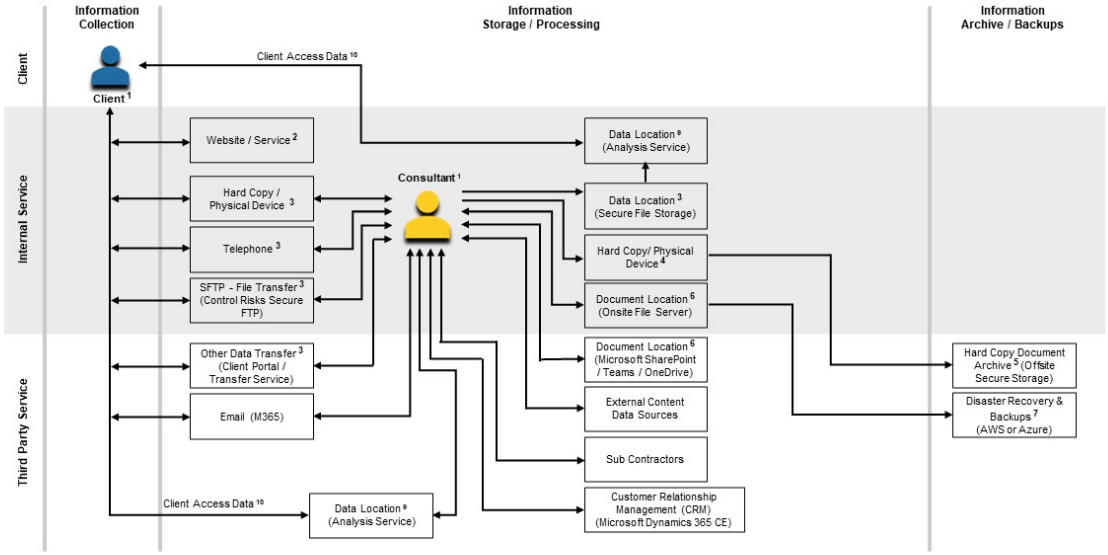


2.3. Forensic imaging, data collection and eDiscovery services (data filtering, processing, analytics, hosting, production and project management) (Control Risks acts as processor)

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.

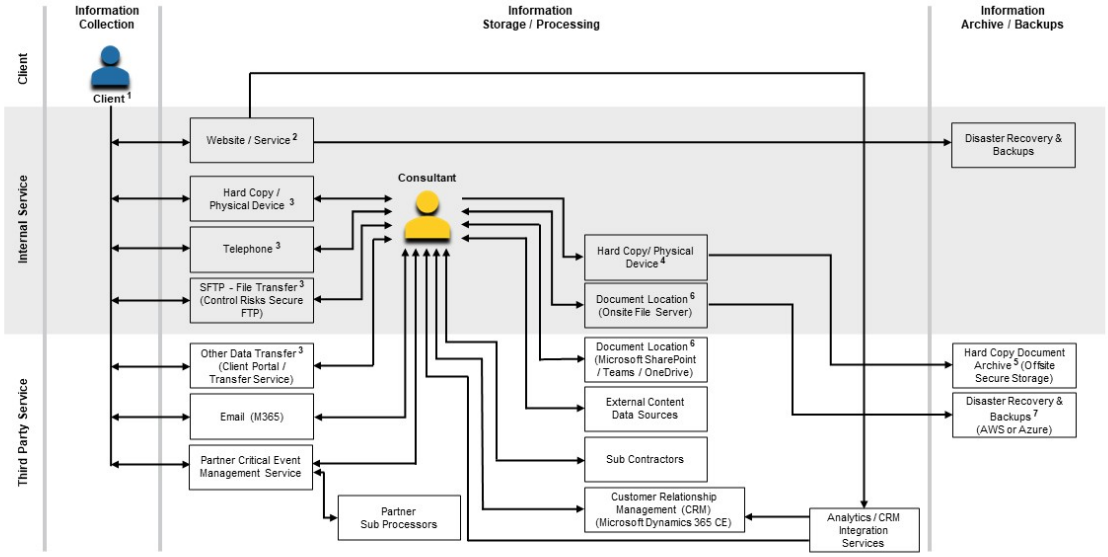
GDPR Data Flow Diagram – 2.3 – Forensic Imaging, Data Collection and eDiscovery Services



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 controller)

In relation to Control Risks Security Consulting Services, 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 fulfil 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.

GDPR Data Flow Diagram – 2.4 – Security Risk Consultancy



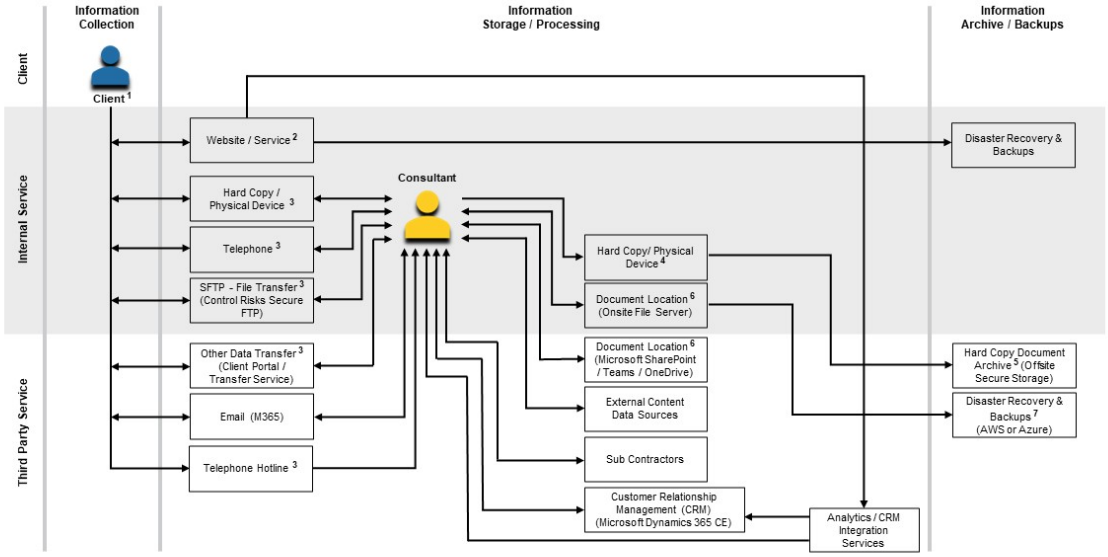
2.5. Protective services, High Risk Managed Services and journey management (Control Risks acts as processor)

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 protective services, High Risk Managed Services and journey management 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.

GDPR Data Flow Diagram – 2.5 Protective Services and Journey Management



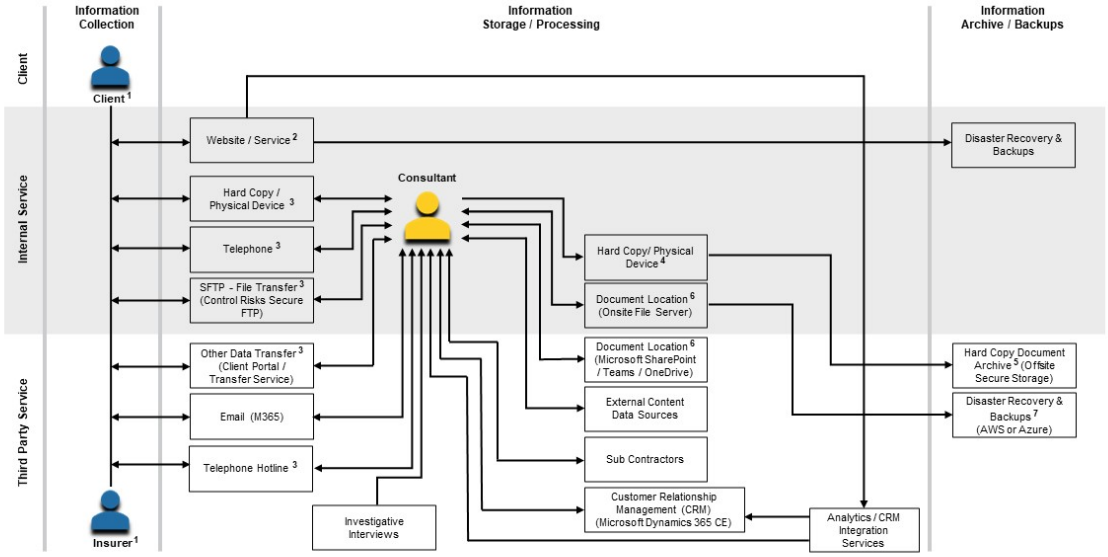
2.6. Cyber Threat Intelligence, Protect and Response Services (Control Risks as a processor other than for source data where Control Risks acts as controller)

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 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 section 2.3 of this document).

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.

GDPR Data Flow Diagram – 2.6 Cyber Threat Assessment Services



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 a call centre provided by a third party supplier) 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.

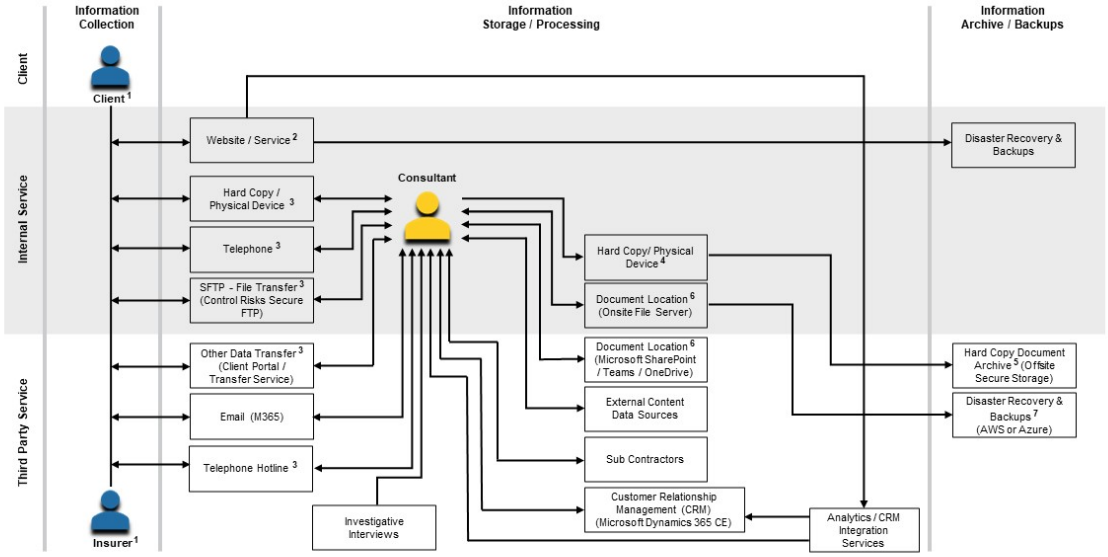
The categories of personal data which are processed are those reasonably required to fulfil the client's request for assistance, such as the data subject's name, age, gender, employment status, address/location, nationality, marital status, contact details (such as telephone and email address), policy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

GDPR Data Flow Diagram – 2.7 Response Services

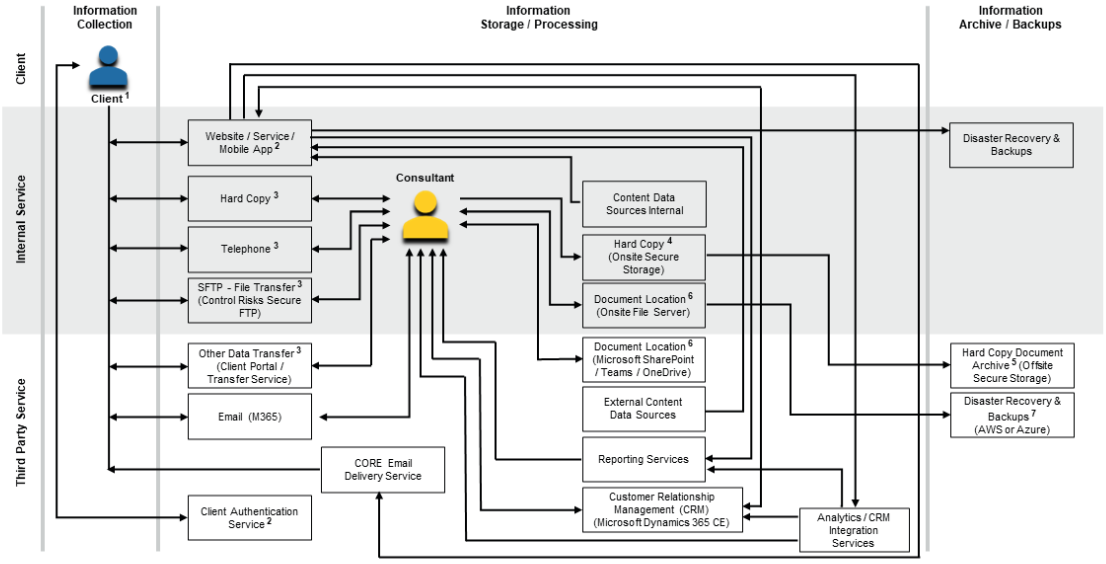


2.8. Seerist and Seerist CORE ("Seerist") (Control Risks, including its subsidiary Seerist, acts as processor)

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 Seerist 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 processor. 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 a controller.

GDPR Data Flow Diagram – 2.8 Seerist and Seerist CORE



2.9. Control Risks ONE (Control Risks acts as a controller or processor)

Control Risks ONE is a subscription-based service providing access to a Control Risks' 24/7 global risks and operations centre ("**G-ROC**") with three levels of service: On Call, On Watch, and On Side. When subscribing to one of the levels, clients are required to supply certain information to enable Control Risks to provide the services; Control Risks is a controller for any personal data collected from the client from the onboarding questionnaires or interviews, as we determine the questions, type, and amount of personal data needed for us to assess the client's needs and risk profile.

Control Risks is generally a processor on behalf of the client for any personal data processed when the client calls into the G-ROC or for any services provided by the G-ROC to the client as personal data processed during the provision of these services is done upon the instructions of the client. Further, Control Risks only processes the data provided by the client for the client's purposes.

Control Risks may retain logs of phone calls and recordings as a controller.

For any other services which the client engages Control Risks as part of its subscription to Control Risks ONE, please refer to the relevant sections above to determine Control Risks status as controller or processor.

GDPR Data Flow Diagram – 2.9 – Control Risks ONE