Privacy & Data Protection Policy

V3.0.2021

Contents

1 Introduction

In our everyday business operations, CalQRisk makes use of a variety of data about identifiable individuals, including data about:

- Current, past and prospective employees
- Visitors and other patrons
- Current, past and prospective service users
- Visitors to our websites
- Marketing subscribers
- Other stakeholders

In collecting and using this data, CalQRisk is subject to a variety of legislation controlling how such activities may be carried out and the safeguards that must be put in place to protect it.

2 Purpose

The purpose of this policy is to set out the relevant privacy and data protection legislation and to describe the steps CalQRisk is taking to ensure that we comply with it.

This control applies to all systems, people and processes that constitute CalQRisk's information systems, including directors, management, employees, suppliers, and other third parties who may be given access to the personal data controlled by CalQRisk.

The following policies and procedures are relevant to this document:

- *GDPR Roles & Responsibilities*
- *End User Licence Agreement*
- *Information Security Policy*
- *Incident Response Plan*
- *Data Subject Request Response Procedures*
- *Personal Data Process Mapping and Data Cataloguing Procedures*
- *Records Retention and Deletion Policy*
- *Data Protection Impact Assessment Process*

3 Privacy and Personal Data Protection Policy

3.1 The General Data Protection Regulation

It is CalQRisk's policy to protect the rights and freedoms of our employees and clients and to ensure that our compliance with the GDPR and other relevant legislation is clear and demonstrable at all times. The General Data Protection Regulation (GDPR) is one of the most significant pieces of legislation affecting the way that CalQRisk carries out its information processing activities.

3.2 Relevant Definitions

The definitions most relevant to this policy are listed in Table 1, below:

Extracted from GDPR – Article 4
Personal Data *means*: *any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person* – Article 4(1)
Processing means*:* *any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction* – Article 4(2)
Controller means*:* *the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or* the *specific criteria for its nomination may be provided for by Union or Member State law* – Article 4(7)
Processor means: *A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller* – Article 4(8)
Third Party means: *A natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data* – Article 4(10)

Table 1 – GDPR definitions

3.3 Principles Relating to Processing of Personal Data

The GDPR is based on a number of fundamental principles; these are set out in Article 5 and summarised in Table 2.

Extracted from GDPR – Article 5
1. Personal data shall be: *(a) processed lawfully, fairly and in a transparent manner* *(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; ('purpose limitation')* *(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');* *(d) accurate and, where necessary, kept up to date; ('accuracy');* *(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; ('storage limitation');*

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

Table 2 – GDPR Data Protection Principles

CalQRisk will take all reasonable steps to ensure that we and our outsourced processors comply with all of these principles both in the processing currently carried out and in the introduction of new methods of processing, such as modifications to or the introduction of new IT systems, outsourced processors, etc.

3.4 The Rights of the Individual

Data Subject rights under the GDPR consist of:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

Each of these rights are supported by appropriate procedures within CalQRisk that allow the required action to be taken within the timescales set out in the GDPR. These timescales are shown in Table 3.

Data Subject Request	Timescale
The right to be informed	When data is collected (if supplied by data subject) or within one month (if not supplied by data subject)
The right of access	One month
The right to rectification	One month
The right to erasure	Without undue delay
The right to restrict processing	Without undue delay
The right to data portability	One month
The right to object	On receipt of objection
Rights in relation to automated decision making and profiling.	Not specified

Table 3 - Timescales for data subject requests

3.5 Lawfulness of Processing

At CalQRisk, it is our policy to identify and designate the appropriate lawful basis for processing personal data and to document it, in accordance with the Regulation. There are six lawful bases and these are briefly described in Table 4, below:

Lawful Bases for Processing: GDPR – Article 6
Consent *Where relying on consent as the legal basis for processing, CalQRisk will always obtain and retain evidence of explicit consent from a data subject to collect and process their data. In respect to children below the age of 16, parental consent will be obtained. We will provide transparent information about our use of personal data to the data subject at the time that consent is sought. We will explain their rights with regard to their data, such as their right to withdraw consent. This information will be provided in an accessible form, written in clear and plain language, and made available free of charge. If personal data is not obtained directly from the data subject then the information will be provided to the data subject within a reasonable period after the data are obtained and not later than one month.*
Performance of a Contract *Where the personal data processing is required to fulfil a contract between CalQRisk and the data subject, explicit consent will not be required. This will often be the case where a contract cannot be completed without the personal data in question – e.g. data required to complete a payment transaction or to process wage payments, etc.*
Legal Obligation *Where the personal data processing is required in order to comply with the law, explicit consent will not be required. This may be the case for some data related to employment and taxation, for example.*
Vital Interests of the Data Subject *Where the personal data processing is required to protect the vital interests of the data subject or of another natural person, this may be used as the lawful basis for the processing. Where this basis is used, CalQRisk will retain reasonable, documented evidence that this is the case. This basis will be used only in extreme circumstances - for instance, in a life or death situation – where the consent of the data subject consent cannot be obtained.*
Task Carried Out in the Public Interest *Where CalQRisk needs to perform a task that it believes is in the public interest or as part of an official duty then the data subject's consent will not be requested. The assessment of the public interest or official duty will be documented and made available as evidence where required.*
Legitimate Interests *If the processing of specific personal data is in the legitimate interests of CalQRisk and is judged not to affect the rights and freedoms of the data subject in a significant way, then this may be relied on as the lawful basis for the processing. The reasoning behind this view will be documented. For example, it may be used to send subscribers to our email newsletter information on events, resources or CalQRisk features and benefits that they are likely to have an interest in, within twelve months of our last*

correspondence. We will also rely on legitimate interests to send previous customers information on similar services, or special offers that they are likely to have an interest in, within twelve months of the last transaction with that customer. Digital marketing is governed by the ePrivacy Regulations, 2011

Table 4 – Lawful Bases for Processing

3.6 Privacy by Design

CalQRisk has adopted the principle of Privacy by Design and has reviewed and appropriately modified our business processes to comply with this element of the GDPR. We will ensure that the definition and planning of all new or significantly changed methods for collecting or otherwise processing personal data will be subject to due consideration of privacy issues, including the completion of data protection impact assessments, where necessary. The use of techniques such as data minimisation and pseudonymisation will be considered where applicable and appropriate.

3.7 Contracts Involving the Processing of Personal Data

CalQRisk will ensure that all personal data processing relationships it enters into are subject to a documented contract that includes, at a minimum, the specific information and terms required by the GDPR. For more information, refer to your End User Licence Agreement.

3.8 International Transfers of Personal Data

It is CalQRisk's policy to process all personal data within the European Union, within reason. Any potential transfers of personal data outside the EU will be carefully reviewed prior to the transfer taking place. This is so that we can ascertain that the receiving third country falls within the limits imposed by the GDPR and that they have appropriate safeguards in place in relation to privacy and personal data protection.

3.9 Data Protection Officer

A defined role of Data Protection Officer (DPO) is required under the GDPR if an organisation is a public authority, if it performs large scale monitoring or if it processes special categories of data on a large scale. The DPO is required to have an appropriate level of knowledge of data protection law and of their organisation's business environment. It can either be an in-house resource or be outsourced to an appropriate service provider.

CalQRisk has evaluated the requirement and decided that the appointment of a Data Protection Officer is not required. The responsibility for data protection has been assigned to the management team. Data protection compliance monitoring is the responsibility of the Managing Director.

3.10 Breach Notification

It is our policy to be fair and proportionate when considering actions to be taken to inform affected parties regarding breaches of their personal data. In line with the GDPR, where a breach is known to have occurred which is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed within 72 hours. This will

be managed in accordance with our Incident Response Plan which sets out the overall process for handling information security incidents.

3.11 Addressing Compliance with the GDPR

The following actions are undertaken to ensure that CalQRisk always complies with the accountability principle of the GDPR:

- The legal basis for processing personal data is clear and unambiguous.
- Appropriate resources have been assigned to the function who has responsibility for data protection in the organisation.
- All personnel involved in handling personal data understand their responsibilities for following good data protection practice.
- Training in data protection is provided to all employees.
- Data protection is part of all new employee induction training.
- The rules regarding consent are followed.
- Routes are available to data subjects wishing to exercise their rights regarding personal data and there are procedures in place to ensure that such requests are handled effectively.
- An Incident and near miss reporting process is in place and is reviewed regularly.
- Regular reviews of procedures involving personal data are carried out.
- Privacy by design is adopted for all new, or significant modifications to, systems and processes.
- The following documentation of processing activities are recorded:
    - Organisation name and relevant details
    - Purposes of the personal data processing
    - Categories of individuals and personal data processed
    - Categories of personal data recipients
    - Agreements and mechanisms for transfers of personal data to non-EU countries including details of controls in place
    - Personal data retention schedules
    - Relevant technical and organisational controls in place

These actions are reviewed on a regular basis as part of the management process concerned with data protection.

Policy Date of Effect: 01/07/2021

Approved By: _____