QUALITY MANAGEMENT SYSTEM

DATA PROTECTION AND PRIVACY NOTICE

Document History

Issue	Date	Status / Changes
1	May 2018	First issue to support the implementation of GDPR.
2	Feb 2019	Role titles changed.
3	May 2019	New ISO 9001 and UKAS Logo added to front page of the procedure.
4	June 2022	QMS Document Rebrand – No change to content
5	May 2023	Minor formatting and singular wording updates
6	March 2024	Annual review. Minor updates.
7	July 2024	Updated to account for use of Kissflow

Table of Contents

COMMITMENT

The Board and Executive Team of React Engineering are fully committed to the protection of your personal data and the implementation of this policy.

Phil Redfern (Managing Director)

1 INTRODUCTION

The Directors and Executive Team of React Engineering recognise the importance of protecting personal data and maintaining personal privacy and understand the potential harm that can result from inappropriate use and distribution of this information. Therefore, we are committed to ensuring the protection of personal data in line with the requirements of the General Data Protection Regulations[1] (GDPR), which classify React Engineering as a Data Controller.

In order to operate our business effectively, we have a need to:

- Store, control and process personal data about several categories of individuals. The principal categories of individuals are:
    - Our employees.
    - Our subcontractors.
    - Our clients.
    - Personnel applying for employment with React Engineering.
    - Personnel providing us with their personal data for other reasons (e.g. in support of our STEM activities).
- Share personal data with third parties. The principal types of third parties are:
    - Organisations we use to support the effective running of our business (e.g. accountants, solicitors, pensions providers, banks).
    - Organisations we have a legal responsibility / requirement to share personal data with (e.g. HMRC).
    - Clients, subcontractors and other organisations (e.g. vetting organisations) required in order for us to deliver work effectively and efficiently.

In our commitment to protecting the personal data that we hold, control, process and share, we fully support the data protection principles and personal rights defined within the GDPR[1].

2 DATA PROTECTION PRINCIPLES

In summary, the data protection principles require that personal data be:

1. Processed lawfully, fairly and in a transparent manner.
2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
4. Accurate and, where necessary, kept up to date.
5. 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.
6. Processed in a manner that ensures appropriate security of the personal data.

The GDPR[1] places a requirement on us to demonstrate compliance with these principles. This policy and the documents referenced from it provide that demonstration.

3 YOUR PERSONAL RIGHTS

The personal rights that are relevant to the personal data held by React Engineering can be summarised as:

1. The right to be informed about the personal data relating to you that we store, control, process and share with third parties.
2. The right of access to the personal data that we hold relating to you.
3. The right to rectification of any personal data relating to you that is incorrect or out-of-date.
4. The right to erasure of your personal data where it is no longer required and in certain other circumstances defined by the GDPR[1] .
5. The right to restrict processing in certain circumstances defined by the GDPR[1].
6. The right to data portability (i.e. the ability to readily move your personal data from one IT system to another with no detriment to usability).
7. The right to object to the processing of your data in certain circumstances defined by the GDPR[1].

4 ACCOUNTABILITY

To ensure that the appropriate level of accountability is in place for the protection of personal data, the Board[2] appointed Finance and Assurance Director / Senior Information Risk Owner as the senior responsible person for the protection of personal data. His contact details are as follows:

Paul Botterill
01946 813778
pbotterill@react-engineering.co.uk

5 WHAT PERSONAL DATA DO WE HAVE, WHY AND WHAT DO WE DO WITH IT?

In order to appropriately protect personal data, it is important to first understand what information we have, what we do with it, who we share it with and what our legal bases for storing, controlling and processing it are. This information is documented in the GDPR Documentation spreadsheet[3], with the underpinning justification for the legal bases documented in Legal Bases of Retaining and Processing Personal Data document[4] (these demonstrate compliance with data protection principles 1, 2, 3 and 5 and supports personal right 1). As and when new types of personal data or different uses for the data are required by the business, the subject of the data will be informed of this requirement before any change is made and these documents will be updated accordingly. We will never obtain new types of personal data about an individual or use an individual's personal data in a manner not included within these documents prior to informing the individual.

6 HOW DO WE PROTECT YOUR PERSONAL DATA?

In order to appropriately protect the personal data that we store, control, process and hold, we have implemented the following robust protective measures:

- The personal data is held on our secure IT network and, for recruitment records on Kissflow online platform. The specific measures and layers of protection that our secure IT network provides are detailed within our Risk Management and Accreditation Document Set[5] (RMADS). The RMADS covers the protection of both client and Government Security Classified information and personal data, both of which require broadly similar levels of protection. Kissflow provides two-factor authentication, access control and data is stored on Amazon Web Services (AWS) and Google Cloud Platform (GCP), both of which are very secure cloud infrastructure.
- We apply access control to the various areas of our IT network so that we can apply the "need to know" principle to all information (including personal data) that we hold.
- The personal data is held within a secure building. Similar to the RMADS, the building is also independently assessed for holding levels of Government Security Classified information
- We implement a Data Protection Procedure[8], which provides "signposts" to where protective measures are specified, defines any additional protective measures required and defines what to do in the event of a data breach.
- We provide training and briefing to our employees on the requirements and responsibilities for protection of information.
- We have contracts and/or letters of engagement with the organisations that we share personal data with that contain, as a minimum, the required clauses set out within GDPR to ensure that they provide suitable protection for any personal data we share with them.
- Our Subcontractor Procedure[9] and Finance Procedure[10] require us to ensure that any new suppliers, with whom we need to share personal data, have the appropriate protections in place.

We recognise and are committed to discharging our responsibilities for protecting personal data. Therefore, we maintain strong protective systems and procedures to ensure the protection of data. More than this, the requirement to protect information is embedded within our culture and our employees understand and continually demonstrate their understanding of the responsibility to protect information. To ensure that this remains current, we will regularly audit our systems and procedures and ensure that our employees are kept up-to-date with their information protection responsibilities.

These protection measures demonstrate compliance with data protection principle 6.

7 DATA PROTECTION PROCEDURE

We maintain and implement a data protection procedure[8] that defines the necessary control measures to ensure protection of personal data. It demonstrates compliance with all data protection principles and how we support all personal rights. This procedure will be regularly reviewed and audited (see references 11, 12 & 13) in order to provide assurance that your personal data is being protected appropriately and to ensure continued relevance and effectiveness of the data protection control measures.

8 REFERENCES

1. GDPR (https://gdpr-info.eu/)
2. January Board Meeting (10/01/2018, A01001/1718/002)
3. GDPR Documentation spreadsheet (A08001/P/019)
4. Legal Bases of Retaining and Processing Personal Data (A08001/P/010)
5. RMADS (A10000/02/001)
6. RMADS Accreditation (A10000/02/001)
7. No longer used
8. Data Protection Procedure. (A08001/P/009)
9. Subcontractor Procedure (A08001/P/065).
10. Finance Procedure. (A08001/P/060)
11. Data Protection Audit (A08001/F/046)
12. Data Deletion Audit. (A08001/F/045)
13. Training Audit. (A08001/F/029)