

# DATA PROTECTION POLICY

## INTRODUCTION

The CDR Group is registered with the Data Protection Act 2018 and registration is renewed annually. Compliance with the Data Protection Act is considered to be of prime importance to the Company and all activities within the scope of the Act are closely monitored.

Responsibility for compliance with the Act rests with the Directors and Managers. Staff are made aware of the importance of complying with the Act as part of their induction procedure. During the course of their work, staff are regularly reminded that any personal details are to be treated as highly confidential and not to be divulged to any other party. Any contravention of this directive would be subject to the Disciplinary Procedure.

The Directors are fully supportive of this policy and expect all staff to conform to the Data Protection Act.

We, Contract Data Research Ltd (trading as CDR Group), hold personal data about our employees, clients, customers, suppliers and other individuals for a variety of business purposes.

This policy sets out how we seek to acquire, process, retain and protect personal data and ensure that staff understand the rules governing their use of personal data to which they have access in the course of their work. In particular, this policy requires staff to ensure that the designated Data Protection Officer (DPO) be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

We process personal data fairly and lawfully in accordance with individuals' rights. This generally means that we should not process personal data unless the individual whose details we are processing has positively consented to this happening.

We adopt the eight principles of data protection, namely:

- Data shall be processed fairly and lawfully
- Data shall be processed only for purpose it was collected
- Data shall be adequate, relevant and not excessive
- Data shall be accurate and up to date
- Data shall be retained no longer than is necessary
- Data shall be processed in accordance with subjects rights
- Data shall be stored securely
- Data shall not be readily transferred outside the EEA

The company has been registered with Data Protection Act 1998 (DPA) since 1999, and in 2018 introduced the requirements of the General Data Protection Regulation 2016 (GDPR) which became effective as from the 25th May 2018.

## DEFINITIONS

### Business purposes

The purposes for which personal data may be used by CDR Group:

Personnel, administrative, financial, regulatory, payroll and business development purposes.

Business purposes include the following:

- Compliance with our legal, regulatory and corporate governance obligations and good practice
- Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests
- Ensuring business policies are adhered to (such as policies covering email and internet use)
- Operational reasons, such as recording transactions, training and quality control, ensuring the confidentiality of commercially sensitive information, security vetting, credit scoring and checking
- Investigating complaints

- Checking references, ensuring safe working practices, monitoring and managing staff access to systems and facilities and staff absences, administration and assessments
- Monitoring staff conduct, disciplinary matters
- Marketing our business
- Maintaining customer care where there is an existing business relationship
- Improving services
- Technical Support requests and analysis

## **Personal data**

Information relating to identifiable individuals, such as job applicants, current and former employees, agency, contract and other staff, clients, suppliers and marketing contacts.

Personal data we gather may include: individuals' contact details, educational background, financial and pay details, details of certificates and diplomas, education and skills, nationality, job title, emergency contact details, details of any known disability and CV.

## **Sensitive personal data**

Personal data about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, criminal offences, or related proceedings. Any use of sensitive personal data should be strictly controlled in accordance with this policy.

## **Data Protection Officer (DPO)**

CDR Group has designated J E Ievers as DPO. He has overall responsibility for the day-to-day implementation of this policy.

## **Supervisory Authority (SA)**

ICO - Information Commissioner's Office.

## **EEA**

European Economic Area.

## **PIA**

Privacy Impact Assessment.

## **SCOPE & RESPONSIBILITY**

This policy applies to all CDR Group staff. They must be familiar with this policy and comply with its terms.

This policy supplements our other policies relating to Internet, email use and handling credit card transactions. We may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be circulated to staff before being adopted.

## **Responsibilities of the Data Protection Officer:**

- Keeping the directors updated about data protection responsibilities, risks and issues
- Reviewing all data protection procedures and policies on a regular basis
- Arranging data protection training and advice for all staff members and those included in this policy
- Answering questions on data protection from staff, board members and other stakeholders
- Creation of a Crisis Team in the event of a serious data breach
- Responding to individuals such as clients and employees who wish to know which data is being held on them by the CDR Group
- Checking and approving with third parties that handle the company's data any contracts or agreement regarding data processing

## **Responsibilities of the IT Manager:**

- all systems, services, software and equipment meet acceptable security standards
- Checking and scanning security hardware and software regularly to ensure it is functioning properly
- Ensure third-party services, such as cloud services which the company uses to store or process data adheres to GDPR

## **Responsibilities of the Sales/Marketing Manager:**

- Approving data protection statements to clients/customers requesting GDPR compliance.
- Addressing data protection queries from clients, target audiences or media outlets
- Co-ordinating with the DPO to ensure all marketing initiatives adhere to data protection laws and the company's Data Protection Policy

## **Responsibilities of all staff when processing data ensure that:**

- Necessary to deliver our services
- In our legitimate business interests and not unduly prejudice the individual's privacy
- In most cases this provision will apply to routine business data processing activities

## **PRIVACY NOTICE**

Being transparent and providing accessible information to individual about how we will use their personal data is important for our organisation. Our web site and Form QM9-1-30 contains a Privacy Notice to clients on data protection.

The notice details how we collect data and what we do with it:

- Who is collecting it
- What information is being collected/held
- How it is collected
- Why it is being collected
- How it will be used
- Who it will be shared with (3rd parties)
- Identify and detail contacts of our DPO
- Details of transfers to third country and safeguards
- Retention period
- Access requests so that customers have a right of access to the personal data that we hold about them

In most cases where we process sensitive personal data we will require the data subject's explicit consent to do this unless exceptional circumstances apply or we are required to do this by law. Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

We will ensure that any personal data we process is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. We will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

Individuals may ask that we correct inaccurate personal data relating to them. Any such changes should be notified to the DPO and recorded.

The individual must take reasonable steps to ensure that personal data we hold is accurate.

## **PRIVACY IMPACT ASSESSMENT**

A PIA will be performed by the DPO and regularly reviewed. This will determine:

- What personal data is held now
- How is the personal data used
- How is the personal data stored
- Identify any sensitive personal data
- Assess risks of existing and new technology
- Assess risks of any software used in house
- Assess risks of any marketing methods

The results of the PIA will be recorded on the data register.

## **PROCESSING CONDITIONS**

We will ensure any processing of personal data is justified and documented. All staff who are responsible for processing personal data will be aware of the conditions for processing. The conditions for processing will be available to data subjects in the form of a privacy notice.

## **PRIVACY BY DESIGN AND DEFAULT**

We adopt the Privacy by Design principles to achieve privacy and data protection compliance. The DPO is responsible for conducting PIA and ensuring that all IT projects commence with a privacy plan. Privacy settings will be set to the most private by default when relevant and when it does not have a negative impact on the data subject.

## **CONSENT**

The data that we collect is subject to active consent by the data subject. This consent can be revoked at any time. Any criminal record checks must also be justified by law. Criminal record checks cannot be undertaken based solely on the consent of the subject.

## **SUBJECT ACCESS REQUESTS**

Individuals are entitled to request access to information held about them. Any such request should be referred to the DPO. The response to the request:

- Will be without undue delay, at least one month of the request (three months if complex).
- Be provided free of charge unless the request is manifestly unfounded or excessive.
- Confirmation as to whether or not their personal data is being processed.
- Information on their data, including the purpose of processing, categories of data collected and the recipients of such data.
- A copy of the data being processed.
- If requested, not to use their personal data for direct marketing purposes.
- If requested, the data subject may request that any information held on them is deleted or removed, (right to be forgotten) and any third parties who process or use the data must also comply with the request

## **POTENTIAL SOURCES OF DATA BREACH**

- Lost or theft of device (printed data, laptop, drive, stick)
- Data transferred to inappropriate third party
- Cyber attack (virus, worm, firewall failure)
- Direct marketing to an individual who has not positively agreed to be approached by us or has opted out.

## **DATA TRANSFER**

There are restrictions on international transfers of personal data. Data must not be transferred outside the EEA without specific consent from the subject and consulting the DPO. There must be a legal contract that stipulates that the non-EEA recipient agrees to the data protection safeguards required.

## **DATA SECURITY**

All personal data will be secured against loss or misuse. Where other organisations process personal data as a service on our behalf, the DPO will establish what, if any, additional data security arrangements need to be implemented in contracts with those third party organisations.

## **DATA STORAGE**

Personal data:

- Stored on printed paper will be kept in a secure place where unauthorised personnel cannot access it.
- Printed data should be shredded when it is no longer needed.
- Stored on a computer should be protected by strong passwords that are changed regularly.
- Stored on portable discs, CD's, DVD's or memory sticks, when not in use, will be kept in a secure place where unauthorised personnel cannot access it.
- Stored on any cloud service must be approved by the DPO
- Stored on servers must be in a secure location and protected by security software and strong firewalls.
- Should be regularly backed-up in accordance with the Company's backup procedures
- Should never be saved directly to mobile devices such as laptops, tablets or mobile phones.

## **DATA RETENTION**

We will retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons that the personal data was initially obtained.

## **DATA REGISTER**

A Data Register, Form QM 9-1-31, will be maintained and will contain information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention time-scales that may be relevant. This register will be initially a result of the PIA, but will be reviewed as required by new marketing initiatives and regularly via the company's QA system.

## **TRAINING**

All staff will receive in-house training on this policy. New joiners will receive training as part of their induction course. Refresher training may be available during weekly meetings. Further training will be provided whenever there is a substantial change in the regulations or our policy and procedures. Completion of training is compulsory.

## **AUDITING**

All staff must observe this policy.

The procedures will be regularly monitored/audited via the company's QA system to monitor data collection and storage methods, manage and mitigate risks and to maintain the data register.

## **CYBER SECURITY**

A Register of Cyber Security Breaches, Form QM9-1-32, is kept of any cyber breach event e.g. Malware attack and the actions/investigations that have taken place to ensure data security, even though no data breach has occurred.

## **FAILURE TO COMPLY**

We take compliance with this policy very seriously. Failure to comply puts the subject, staff member and the organisation at risk.

The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under our procedures, which may result in dismissal.

Penalties for non-compliance under GDPR are high: businesses can be fined up to 20 million Euros or 4% of global annual turnover.

If you have any questions or concerns about anything in this policy, do not hesitate to contact our DPO.

## **DATA BREACH ACTIONS**

All members of staff have an obligation to report actual or potential data protection compliance failures to the DPO. This allows the company to:

- Investigate the process failure, actual consequences and take remedial steps if necessary
- Maintain a register of compliance failures
- Notify the Supervisory Authority (SA) within 72 hours of any compliance failures that are material either in their own right or as part of a pattern of failures where there is a risk to the rights and freedoms of the subjects
- Notify the subjects concerned of any personal data compromised if there is a high risk to the rights and freedoms of the subjects