

## **DEBBIEJUDDHR LIMITED** **DATA PROTECTION POLICY**

In keeping with debbiejuddhr Limited's other policies and procedures, this document is issued for guidance and is not intended to have contractual effect. debbiejuddhr reserves the right to vary, amend or depart from the contents of this policy and procedure from time to time in appropriate circumstances.

### **1.0 Policy**

debbiejuddhr is committed to protecting confidential data, personal data and personal sensitive data and to meeting the legal requirements of the Data Protection Act 2018.

debbiejuddhr will comply with the rules of good information handling, known as the data protection principles under the Data Protection Act. In line with these principles, debbiejuddhr will ensure that all personal data is:

- collected and processed fairly and lawfully in order to meet operational needs, or fulfil legal requirements;
- obtained only for one or more specified and lawful purposes;
- adequate, relevant and not excessive;
- accurate and where necessary kept up-to-date;
- not kept for longer than necessary;
- processed in accordance with the individual's rights under the Data Protection Act;
- kept secure;
- not transferred outside the European Economic Areas unless the country offers adequate data protection.

debbiejuddhr will hold and process, both electronically and manually, the personal data and sensitive personal data it collects in relation to both its own employees and associates and also the employees of debbiejuddhr clients and their employment, for the purposes of the provision of human resources advice and support and/or for compliance with applicable procedures, laws and regulations.

debbiejuddhr will follow both the client's data protection policy and the debbiejuddhr data protection policy when dealing with client confidential data, personal data and personal sensitive data.

debbiejuddhr has appointed a Data Controller who is responsible for data protection compliance and provides a point of contact for all data protection issues. The Data Controller is responsible for the operation of this policy. debbiejuddhr will ensure that all employees and associates follow this policy and are made aware of good practice in data protection.

## 2.0 Scope

This policy applies to all employees of debbiejuddhr.

This policy also applies to all associates of debbiejuddhr and to all employees and workers employed by suppliers, contractors and agents acting for, or on behalf, of debbiejuddhr.

## 3.0 Relevant Legislation

### 3.1 The Data Protection Act 2018 (DPA 2018) and The UK General Data Protection Regulation (GDPR 2021)

The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR). The Data Protection Act 2018 (DPA) is the main UK legislation governing data protection.

The DPA 2018 sets out the framework for data protection law in the UK. It updates and replaces the Data Protection Act 1998, and came into effect on 25 May 2018.

The GDPR 2021 is based on the EU GDPR ([General Data Protection Regulation \(EU\) 2016/679](#)) which applied in the UK before that date, with some changes to make it work more effectively in a UK context.

The GDPR 2021 sets out UK law and includes the key principles, rights and obligations for most processing of personal data in the UK. Separate data protection rules for law enforcement authorities, extends data protection to some other areas such as national security and defence.

The DPA 2018 and UK GDPR 2021 sits alongside and supplements each other for example by providing exemptions.

The legislation gives individuals rights concerning the processing of personal data and access information held about them. In addition, there are obligations for better data management and a regime of fines. The legislation applies to personal data in a computerised format, as part of an accessible record or held manually as part of a relevant filing system.

The legislation is overseen and enforced by the Information Commissioners Office (ICO), which is an independent public body responsible directly to Parliament.

### 3.2 The Telecommunications (Lawful Business Practice) Regulations 2000

These UK regulations were issued under the Regulation of Investigatory Powers Act 2000 to comply with the EU's Telecommunications Data Protection Directive and cover all types of telecommunications (telephone, email, fax, etc) on public and private systems.

## 4.0 Definitions

**Data Controller:** debbiejuddhr has appointed Laura Turnbull as the debbiejuddhr Data Controller. The Data Controller decides how and why personal data and sensitive personal data is processed and who must comply with certain data protection principles.

**Data Subject:** all living individuals about whom data is processed (employees, workers, applicants of debbiejuddhr and the employees, workers, applicants of debbiejuddhr clients).

**Data Processor:** any person who processes personal data and personal sensitive data on behalf of a data controller. debbiejuddhr acts as a data processor for our clients when handling client personal data and personal sensitive data.

**Data Users:** debbiejuddhr employees and associates whose work involves using personal data.

**Personal Data:** any data from which a living individual (subject) can be identified. This includes personal data stored in both electronic and manual (paper based) records, where the records are structured, accessible and form part of a relevant filing system (filed by subject, reference, dividers or content) and where individuals can be identified. Personal data includes statements of fact; any expression of opinion about an individual; information contained in personnel records, including sickness absence, performance appraisals, salary, and recruitment notes; photographs; minutes of meetings; reports; emails; file notes; handwritten notes; 'post it' notes; CCTV footage where an individual can be identified by the footage.

**Sensitive Personal data:** includes information about an individual's race, ethnicity, political opinion, religious or similar beliefs, trade union membership, health, sex life or any offence committed or alleged to have been committed by that individual. Financial data is also treated as 'sensitive personal data'.

**Processing Information or Data:** any activity that involves the use of the data, namely: obtaining, recording, holding or carrying out any operation on data, including organising, amending, retrieving, using, disclosing, erasing or destroying data. Processing also includes transferring personal data and personal sensitive data to third parties.

## 5.0 Principles

In order to ensure that personal data and personal sensitive data is not kept for longer than necessary, appropriate retention periods for personal data and personal sensitive data will be adhered to, outlined in Appendix A.

Appropriate and adequate security measures will be implemented to protect personal data and personal sensitive data.

All employees and associates responsible for personal data and personal sensitive data will receive appropriate training.

All queries about data protection, internal and external to the organisation will be dealt with effectively and promptly.

## 6.0 Responsibility

### 6.1 Data Controller

debbiejuddhr has appointed Laura Turnbull as the debbiejuddhr Data Controller.

The Data Controller will decide how and why personal data and personal sensitive data is processed, who must comply with certain data protection principles, assess the current knowledge of data protection within debbiejuddhr, manage any security breaches and ensure that appropriate training on data protection is provided to data users, as required.

The Data Controller is also responsible for this policy. Any questions or concerns about the operation of this policy should be referred in the first instance to:

Mrs Laura Turnbull, Email: [laura.turnbull@debbiejuddhr.co.uk](mailto:laura.turnbull@debbiejuddhr.co.uk) Mobile: 079426 039488

### 6.2 Directors

Directors will:

- understand clearly this data protection policy and ensure that this is communicated to all data users;
- support data users in their work involving personal and/or sensitive personal data and personal sensitive data ensuring data users receive appropriate training.

### 6.2 Employees and Associates

Employees and associates will:

- fully understand and comply with this data protection policy;
- have a responsibility under the Data Protection Act to ensure that their activities comply with the data protection principles and have responsibility for the type of personal data and personal sensitive data they collect and how they use it;
- consider and protect, at all times, the security of debbiejuddhr and debbiejuddhr client confidential data, personal data and sensitive personal data and documentation, assessing the physical security of documentation, network security and the security of computer systems and files in order to prevent unauthorised access;

- ensure that personal data and personal sensitive data is not kept for longer than necessary, and that the relevant retention periods outlined in Appendix A are adhered to;
- not disclose confidential data, personal data and sensitive personal data outside the organisation's procedures;
- use personal data held on others for their own purposes; and
- not engage in the misuse of data.

## 7.0 Data Security

debbiejuddhr will ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data and personal sensitive data, and against the accidental loss of, or damage to, personal data and personal sensitive data.

In maintaining data security, debbiejuddhr will guarantee:

- **Confidentiality** - only people who are authorised to use the data can access it
- **Integrity** - personal data and personal sensitive data will be accurate and suitable for the purpose for which it is processed
- **Availability** - authorised users have access to the data they require for authorised purposes.

## 8.0 Data Processors

8.1 Where debbiejuddhr acts as a data processor on behalf of a client, debbiejuddhr will process such data in accordance with the instructions of the client's data controller.

8.2 debbiejuddhr will write to any third party contracted to provide a service for debbiejuddhr which involves the processing of confidential data (such as a payroll processor) and confirm that the third party:

- acts only on the instructions of debbiejuddhr and processes personal data and personal sensitive data only connection with the provision of the services;
- shall not disclose or divulge confidential data to any person other than to officers or employees of the Client; and
- shall comply with any code of practice or guidance in respect of the Data Protection Acts, relevant EU Directives, and the General Data Protection Regulation 'GDPR' (from time to time in force, which may include eg erasing or preserving confidential data.

## 9.0 Telecommunications

debbiejuddhr management will intercept debbiejuddhr telecommunications without consent:

- to establish facts;
- to find out if a communication is for business or private purpose;

- for quality control or training;
- to comply with regulatory or self-regulatory procedures;
- for system maintenance;
- to detect unauthorised use;
- to prevent or detect crime; and
- for national security purposes.

## **10.0 Access to Personal Data Information**

Subject to certain exceptions, under the Data Protection Act 2018, individuals are entitled to have access to personal data held about them by debbiejuddhr. debbiejuddhr will charge a £10 fee for supplying employees with their personal data.

Anyone wishing to access their personal data should contact the Data Controller in writing, providing sufficient detail to enable the requested data to be identified and include the £10 fee. Once the detail has been received enabling the requested data to be clearly identified, the information will be supplied within 40 days.

## **11.0 The Information Commissioner's Office (ICO)**

debbiejuddhr has voluntarily registered with the ICO. Registration Reference: ZA819942

## **12.0 Failure to Comply**

debbiejuddhr recognises and understands that the consequences of failure to comply with the requirements of the Data Protection Act may result in: criminal and civil action; fines and damages; personal accountability and liability; suspension/withdrawal of the right to process personal data by the ICO; loss of confidence in the integrity of debbiejuddhr's systems and procedures; and/or irreparable damage to the debbiejuddhr's reputation.

Where the individuals outlined in the scope do not comply with this policy, debbiejuddhr may consider taking action in accordance with the debbiejuddhr's disciplinary procedure.

## **12.0 Complaints**

If you consider that debbiejuddhr has not followed this policy, you should contact the debbiejuddhr Data Controller.

Mrs L Turnbull  
Data Controller  
debbiejuddhr Limited  
22 The Drive  
Shotley Bridge  
Consett  
Co Durham  
DH8 0DL

Mobile: 07426 039488

Email: [laura.turnbull@debbiejuddhr.co.uk](mailto:laura.turnbull@debbiejuddhr.co.uk)

### **13.0 Monitoring and Review**

This policy and procedure will be monitored and reviewed annually by the Data Controller. Where there are issues with the way the policy and/or procedure are working, these will be looked at closely with a view to identifying measures to improve their effectiveness.

Document created:	1 September 2021
Last updated:	1 September 2021
Date of next review:	September 2023

## DATA RETENTION PERIODS

### Employees/Workers/Associates

<b>Record Type</b>	<b>Retention Period</b>
Personnel record	Erased 6 years after the date of the termination of employment.
Payroll wage/salary records (also overtime, bonuses, expenses)	Payroll data is held by a third party provider, which has its own Data Protection Policy which applies. The statutory retention period is 6 years from the end of the tax year to which they relate.
Accident books, accident records/reports	Erased 3 years from the date of the last entry (or, if the accident involves a child/young adult, then until that person reaches the age of 21).
Occupational Health electronic and hardcopy documents containing personal and sensitive data.	Erased in line with the occupational health provider's data protection and retention policy and procedure.
Recruitment and selection documentation	Erased 6 months after selection event.

### Current Clients

<b>Record Type</b>	<b>Retention Period</b>
Electronic and hardcopy documents containing personal and sensitive data	Erased 6 months after a case has been completed.
Occupational Health electronic and hardcopy documents containing personal and sensitive data.	Erased in line with the occupational health provider's data protection and retention policy and procedure.

### Ex-Clients

<b>Record Type</b>	<b>Retention Period</b>
Electronic and hardcopy documents containing personal and sensitive data.	Erased 6 months after a case has been completed.
All other electronic and hardcopy documents.	Erased 6 months after a client contract ends.
Occupational Health electronic and hardcopy documents containing personal and sensitive data.	Erased in line with the occupational health provider's data protection and retention policy and procedure.

### Document Record



<b>Version</b>	<b>Date</b>	<b>Reason for Update</b>	<b>Amended By</b>	<b>Approved By/Date</b>
1.0	01.09.21	Created	DJ	DJ – 02.09.21
2.0				