Policy Document

Data Protection

Reed Business School

Introduction

This Policy sets out how Reed processes personal data (in compliance with the Data Protection Act 2018) of its clients, candidates, suppliers, co-members and other third parties.

This Policy applies to all Personal Data processed by Reed regardless of how that data is stored or how old it is.

Although Reed is responsible for what happens to the Personal Data in its control, co-members are also responsible for their own actions when handling Personal Data. Compliance with this Policy is compulsory, as is annual training on the appropriate handling of Personal Data. Any breach of this Policy may result in disciplinary action.

Reed has an appointed a Data Protection Officer ("DPO"). The DPO is responsible for overseeing this Policy, developing related policies and advising on data protection matters.

Document Control

Version:	#08	Approved:	Magdalena Robinson
Date of review:	18.06.2025	Title:	Operations Manager
Next review:	17.05.2026	Signed:	
Author(s):	Emily Dewar		

Personal Data

Personal Data is any data that relates to a living individual or from which a living individual can be identified.

Personal Data which includes information revealing an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health, sex life or sexual orientation, biometric or genetic data, or details of criminal convictions is classified as sensitive personal data.

All of the information that Reed holds about candidates, co-members, managers and referees will constitute personal or sensitive personal data for the purposes of data protection legislation, and Reed's ability to use or hold that information is subject to that legislation.

The penalties for not complying with the legislation includes a maximum fine of up to 20 million Euros (approx. £18 million) or 4% of a company's global turnover and prison sentences. It is therefore vitally important that co-members understand their own, and Reed's, obligations to handle personal and sensitive personal data appropriately.

Data Protection Principles

Personal data must be processed (any use by Reed of personal or sensitive personal data constitutes 'Processing' for the purposes of the legislation), in accordance with the following 8 principles:

Lawfulness, Fairness and Transparency

Reed can only process personal and sensitive personal data for specified lawful purposes which it notifies to data subjects in advance of collecting their personal data.

The most common grounds justifying the processing of personal data are that:

- the data subject has given their consent;
- the processing is necessary for the performance of a contract with the data subject;
- to meet our legal compliance obligations;
- to protect a data subject's vital interests; or
- to pursue our legitimate interests for purposes which do not prejudice the interests or fundamental freedoms of data subjects.

Sensitive personal data receives greater protection than personal data and it may only be processed if the data subject has given consent or if the processing is necessary to comply with obligations imposed on Reed by law.

Consent will not normally be appropriate to cover Reed's recruitment activities, as in order to be valid such consent has to be freely given, which means that it cannot be a condition of accessing our recruitment services.

However, Reed has to be able to process candidate personal data in order to provide its services to them and, as it does not have a contract with candidates and only processes their personal data in order to provide the recruitment services they register for, Reed processes most candidate data because it is in our legitimate interests to do so and does not result in any prejudice to the candidates.

If Reed is required to process sensitive personal data, perhaps to comply with an obligation in the Conduct Regulations which require us to check a candidate's criminal record, that particular processing is carried out because we are legally obliged to.

Similarly, if Reed needs to process personal or sensitive personal data of candidates or co-members to discharge its duties as an employer, then that is the basis on which that processing activity is carried out.

Details of our data processing activities must be provided to candidates when they register with Reed (in the Privacy Notice), to co-members as part of their induction process and to client managers as part of our contract/terms of business with the relevant client.

Any co-members who are concerned or are unsure about the basis on which they or anyone else is processing personal or sensitive personal data should contact the DPO immediately.

Purpose Limitation

Personal data must only be collected and used for the legitimate purposes set out above and of which we must have notified data subjects in advance.

Personal data cannot be used for new or different purposes to the ones we have disclosed to data subjects (for instance to candidates in the Privacy Notice). If a co-member wants to introduce a new product or process which involves handling personal data differently it may be necessary to complete a Data Protection Impact Assessment. To do this you will need to contact: compliance.escalations@reed.com

Data Minimisation

The personal data that Reed collects must be adequate, relevant and limited to what is necessary for Reed to provide its services. If personal data is not relevant to those purposes, Reed should not be collecting it and co-members should not ask for it.

Accuracy

Personal data must be kept accurate and up to date. As soon as a co-member becomes aware that personal data, whether held electronically or otherwise, is out of date, it must be updated and corrected without delay.

Storage Limitation

Personal data must not be kept any longer than is necessary. Reed has a Data Retention and Destruction Policy which applies to all of the information (including personal data) and records must be processed strictly in accordance with that policy (which can be found on the intranet under Consultant tools > Policies.

Security, Integrity and Confidentiality

Personal data must be secured by appropriate technical and organisational measures. Reed's IT Department is responsible for ensuring the security of all data that is held electronically and it is important that Co-members use those IT facilities for processing personal data.

Co-members should not need to process personal data outside Reed's IT systems. However if the use of temporary spreadsheets or other hard copy documents is essential, the documents must not leave the office and must be securely destroyed as soon as they are no longer needed.

Co-members must maintain the security of personal data by following all procedures and technologies that Reed puts in place to ensure the security of personal data from the point of collection to the point of destruction.

Transfer Limitation

Personal data must not be shared with anyone outside Reed unless it is a part of the standard recruitment process and the person to whom that data relates knows that we are likely to do so.

For example, candidates will expect Reed to share their personal data with prospective employers or hirers, but they will not expect us to seek references from their current employers without obtaining their permission.

Co-members must also ensure that personal data is only transferred to third party service providers who agree to comply with the appropriate policies or put adequate measures in place. These should be reflected in our contracts with any such third parties, and queries should be addressed, in the first instance, to the Compliance Team using the email address: compliance.escalations@reed.com

Data Subject's Rights and Requests

All data subjects, including candidates and client contacts, have rights when it comes to what Reed does with their personal data. These include the right to ask us to stop processing their personal data or to delete it, to be given a copy of the personal data that we hold, to prevent us using their personal data for marketing or to complain to the Information Commissioner if they are unhappy with our data processing activities.

If a co-member receives a request from a candidate or client to do something with their personal data, that request must be dealt with immediately. If it is a request to unsubscribe from Reed's services, that should be done at once. If it involves something more unusual, such as deleting them from the database completely or amending the Privacy Notice given to candidates, that request should be passed to the Compliance Team immediately using the email address: compliance.escalations@reed.com

Data subject access requests should also be passed on to the Compliance department immediately using the same email address as also should requests for information (RFIs) from external enforcement agencies such as the police or local authorities.

Data Breaches

Any breach or suspected breach of personal data must be immediately reported to Reed's Data Protection Officer using the email address: data.breach@reed.com

A personal data breach is anything which could compromise the security, confidentiality, integrity or availability of personal data or the physical, technical, administrative or organisational safeguards which we put in place to protect personal data.

As a result, personal data breaches do not just include the unauthorised access or disclosure of personal data because of a hack or if a device or paper file containing personal data is lost or stolen.

If we lose the ability to access personal data either because of a systems problem or because it is accidentally destroyed, that is also likely to be a breach of personal data; as is accidentally sending clients information that they should not see, such as the results of a criminal records check.

Reed is under an obligation to inform the appropriate government regulators of personal data breaches within 72 hours of becoming aware of them and, as a result, co-members must not take time to investigate data breaches before reporting them and must notify the DPO as soon as they become aware of a potential data breach.

Audit and Training

Adherence to this and to related policies will be checked as part of Reed's regular audit process, as is completion of annual training on data protection which is available through LMS365.

Co-members must ensure that they complete the appropriate training, as well as reviewing this and the following related policies:

- Data Retention and Destruction Policy
- Data Protection Impact Assessment Policy
- Subject Access Request Policy
- Co-member Referencing and Vetting Policy
- Bring Your Own Device User Policy
- IT Policy
- RSR Corporate Mobile Device Policy

Complaints and Queries

Data Breaches must always be reported immediately using the email address: data.breach@reed.com

Queries relating to data protection (including data subject access requests) should be addressed to the Compliance Team: compliance.escalations@reed.com

Terms & Conditions
www.reedbusinessschool.co.uk/terms-and-conditions

Reed Business School
The Manor, Little Compton
Moreton-in-Marsh
Gloucestershire GL56 ORZ

01608 674224
rbs.reed@reedbusinessschool.co.uk
www.reedbusinessschool.co.uk