Name of policy	Data Protection Policy
Responsibility for policy	Nicholas Thomas (Data Protection Officer)
Date last reviewed	September 2023
Date of next review	September 2025
Associated policies and documents	Data Retention Policy Information Management and Security Policy

Data protection policy

1. Introduction

1.1 Pearcelegal is a law firm and we provide legal advice and assistance to our clients. We are authorised and regulated by the Solicitors Regulation Authority. The personal data that Pearcelegal processes to provide these services relates to our clients and other individuals as necessary, including staff and suppliers' staff.

1.2 This policy sets out Pearcelegal's commitment to ensuring that any processing of personal data by us, is carried out in compliance with data protection law. Its purpose is also to ensure that staff understand and comply with the rules governing the collection, use and deletion of personal information to which they may have access in the course of their work.

1.3 We are committed to complying with our data protection obligations, and to being concise, clear and transparent about how we obtain and use personal information and how (and when) we delete that information once it is no longer required.

2. Responsibilities

2.1 The Directors have ultimate responsibility for data protection. Nicholas Thomas is the data protection officer and is responsible for informing and advising the practice and its staff on its data protection obligations, and for monitoring compliance with those obligations and with the practice's policies.

2.2 If you have any questions or concerns about this policy or if you need further information, then you can contact the data protection officer in the following ways:

Post: 2 The Square, Solihull, B91 3RB
Email: nicholasthomas@pearcelegal.co.uk
Telephone: 0121 270 2701

3. Scope

3.1 This policy applies to all personal data processed by Pearcelegal and is part of our approach to compliance with data protection law.

3.2 We will ensure that all staff who handle personal data on our behalf are aware of their responsibilities under this policy and other relevant data protection and information security policies, and that they are adequately trained and supervised.

3.3 Breaching this policy may result in disciplinary action for misconduct, including dismissal. Obtaining (including accessing) or disclosing personal data in breach of our data protection policies may also be a criminal offence.

4. Data protection principles

4.1 Pearcelegal complies with the data protection principles set out below. When processing personal data:

- we will process personal data lawfully, fairly and in a transparent manner;
- we will collect personal data for specified, explicit and legitimate purposes only and will not process it in a way that is incompatible with those purposes;
- we will only process the personal data that is adequate, relevant and necessary in relation to the purposes for which it is processed;
- we will keep accurate and up-to-date personal data, and take reasonable steps to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay;
- we will keep personal data in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed; and
- we will process personal data 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.

4.2 Pearcelegal will facilitate any request from a data subject who wishes to exercise their rights under data protection law as appropriate, always communicating in a concise, transparent, intelligible and easily accessible form and without undue delay.

5. Process and procedures

5.1 Pearcelegal will:

- ensure that the legal basis for processing personal data is identified in advance and that all processing complies with the law;
- not do anything with personal data that an individual would not expect given the content of this policy and the fair processing or privacy notice;
- ensure that appropriate privacy notices are in place advising staff and others how and why their data is being processed, and, in particular, advising data subjects of their rights;
- only collect and process the personal data that it needs for purposes it has identified in advance;
- ensure that, as far as possible, the personal data it holds is accurate, or a system is in place for ensuring that it is kept up to date as far as possible;
- only hold on to personal data for as long as it is needed, after which time the practice will securely erase or delete the personal data (the practice's data retention policy sets out the appropriate period of time);

- ensure that appropriate security measures are in place to ensure that personal data can only be accessed by those who need to access it and that it is held and transferred securely.

5.2 Pearcelegal will ensure that all staff who handle personal data on our behalf are aware of their responsibilities under this policy and other relevant data protection and information security policies, and that they are adequately trained and supervised.

5.3 Breaching this policy may result in disciplinary action for misconduct, including dismissal. Obtaining (including accessing) or disclosing personal data in breach of the practice's data protection policies may also be a criminal offence.

6. Data subject rights

6.1 Pearcelegal has processes in place to ensure that we can facilitate any request made by an individual to exercise their rights under data protection law. All staff have received training and are aware of the rights of data subjects. Staff can identify such a request and know who to send it to.

6.2 All requests will be considered without undue delay and within one month of receipt as far as possible.

6.2.1 Subject access: the right to request information about how personal data is being processed, including whether personal data is being processed and the right to be allowed access to that data and to be provided with a copy of that data along with the right to obtain the following information:

- the purpose of the processing;
- the categories of personal data;
- the recipients to whom data has been disclosed or which will be disclosed;
- the retention period;
- the right to lodge a complaint with the Information Commissioner's Office;
- the source of the information if not collected direct from the subject; and
- the existence of any automated decision making.

6.2.2 Rectification: the right to allow a data subject to rectify inaccurate personal data concerning them.

6.2.3 Erasure: the right to have data erased and to have confirmation of erasure, but only where:

- the data is no longer necessary in relation to the purpose for which it was collected; or
- consent is withdrawn; or
- there is no legal basis for the processing; or
- there is a legal obligation to delete data.

6.2.4 Restriction of processing: the right to ask for certain processing to be restricted in the following circumstances:

- if the accuracy of the personal data is being contested; or
- if our processing is unlawful but the data subject does not want it erased; or
- if the data is no longer needed for the purpose of the processing but it is required by the data subject for the establishment, exercise or defence of legal claims; or
- if the data subject has objected to the processing, pending verification of that objection.

6.2.5 Data portability: the right to receive a copy of personal data which has been provided by the data subject and which is processed by automated means in a format which will allow the individual to transfer the data to another data controller. This would only apply if the practice was processing the data using consent or on the basis of a contract.

6.2.6 Object to processing: the right to object to the processing of personal data relying on the legitimate interests processing condition unless the practice can demonstrate compelling legitimate grounds for the processing which override the interests of the data subject or for the establishment, exercise or defence of legal claims.

7. Special category personal data

7.1 This includes personal data revealing or concerning the following:

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- genetic data and biometric data for the purpose of uniquely identifying a natural person;
- an individual's health;
- a natural person's sex life or sexual orientation;

7.2 Pearcelegal processes special category data of clients and third parties as is necessary to provide legal services for the establishment, exercise or defence of legal claims.

7.3 Pearcelegal processes special category data of employees as is necessary to comply with employment and social security law. This policy sets out the safeguards we believe are appropriate to ensure that we comply with the data protection principles set out above. Pearcelegal also has a Data Retention Policy which sets out how long special category data will be held for.

8. Data breaches

8.1 A data breach may take different forms, for example:

- loss or theft of data or equipment on which personal data is stored;
- unauthorised access to or use of personal data by either a member of staff or a third party;
- loss of data resulting from an equipment or systems (including hardware and software) failure;
- human error, such as accidental deletion or alteration of data;
- unforeseen circumstances, such as a fire or flood;
- deliberate attacks on IT systems, such as hacking, viruses or phishing scams; and
- 'blagging' offences, where information is obtained by deceiving the organisation which holds it.

8.2 Pearcelegal will:

- make the required report of a data breach to the Information Commissioner's Office without undue delay and, where possible within 72 hours of becoming aware of it, if it is likely to result in a risk to the rights and freedoms of individuals; and

- notify the affected individuals if a data breach is likely to result in a high risk to their rights and freedoms and notification is required by law.

9. Data protection privacy impact assessment

9.1 Where processing of personal data is likely to result in a high risk to an individual's data protection rights (e.g., where the practice is planning to use a new form of technology), we will, before commencing the processing, carry out a data protection privacy impact assessment to assess:

- whether the processing is necessary and proportionate in relation to its purpose;
- the risks to individuals; and
- what measures can be put in place to address those risks and protect personal data.

9.2 Before any new form of technology is introduced, the employee responsible should therefore contact the data protection officer in order that a data protection privacy impact assessment can be carried out.

9.3 During the course of any data protection privacy impact assessment, the practice will seek the advice of the data protection officer and the views of any other relevant stakeholders.

10. Data retention and storage

10.1 Personal data (and special category personal data) will be kept securely in accordance with our Information Management and Security Policy.

10.2 Personal data (and special category personal data) should not be retained for any longer than necessary. The length of time over which data should be retained will depend upon the circumstances, including the reasons why the personal data was obtained. Pearcelegal retains personal information in order to comply with regulatory and statutory requirements including being able to carry out conflict searches for future matters. Where there is any uncertainty, staff should consult the data protection officer.

10.3 Personal data (and special category personal data) that is no longer required will be deleted permanently from our information systems and any hard copies will be destroyed securely.

11. Cybercrime

11.1 Cybercrime is a crime that has some kind of computer or cyber aspect to it. It takes shape in a variety of forms, e.g., hacking, phishing, malware, viruses or ransom attacks.

Cybercrime raises a number of important issues for the practice, including:

- cost;
- breach of confidentiality or obligations under the data protection regime;
- the potential for regulatory breach;
- reputational damage;
- business interruption;
- structural and financial instability

11.2 All staff must ensure they are familiar with the risks presented by cybercrime and cybersecurity attacks or failures and take appropriate action to mitigate the risks by taking a sensible approach, e.g., not forwarding chain letters or inappropriate/spam emails to others.

11.3 Pearcelegal will help staff by continually raising awareness of those risks and providing regular training:

- at induction;
- refresher training as appropriate;
- when there is a change to the law, regulation or our policy;
- where significant new threats are identified;
- in the event of an incident affecting the firm or a competitor.

11.4 Cybercrime concerns may arise at any time and staff are encourage to report any concerns that they have to Nicholas Thomas.

12. Training

12.1 Pearcelegal will ensure that staff are adequately trained regarding their data protection responsibilities. Individuals whose roles require regular access to personal data, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

13. Monitoring and review

13.1 In order to ensure that it remains fit for purpose, this policy will be formally reviewed at least every two years by the person responsible, as named above.

