



The General Data Protection Regulation and the UK Data Protection Act 2018

A Policy on Retention, Security & Disposal of Personal Data

TWO Ltd has a responsibility to protect the integrity and confidentiality of the personal data held about its clients. Staff have an obligation to ensure that personal data, whether it is oral, printed, hand-written, computer based or however recorded or held is not disclosed to persons who have no right to have access to it.

This policy has been written to provide the necessary guidance to staff detailing their individual responsibilities under the General data Protection Regulation (GDPR) and the Data Protection Act 2018 (the Act) and record retention procedures.

“Personal data” means any information relating to a “natural person” that is an identified or identifiable living individual.

Personal data must be:

- (a) processed fairly and lawfully;
- (b) processed for limited purposes and in an appropriate way and not in anyway incompatible to the purpose for which it was collected;
- (c) adequate, relevant and not excessive for the purpose;
- (d) accurate and kept up to date;
- (e) not kept longer than necessary for the purpose for which it was gathered;
- (f) processed in line with data subjects’ rights;
- (g) kept securely;
- (h) not transferred to people or organisations situated in countries outside the EEA without adequate protection.

A data subject is entitled to:

- (a) request access to any data held about them by a data controller;
- (b) prevent or block the processing of their data;
- (c) ask to have inaccurate data rectified or erased;

- (d) object to processing that is based on the data controller's legitimate interests;
- (e) have their personal data disposed of securely;
- (f) access to the personal data being processed (with limited restrictions);
- (g) request the deletion or removal of personal data in certain circumstances (the right to be forgotten);
- (h) restrict processing of personal data e.g. where they contest its accuracy or object to the processing;
- (i) data portability - to provide their personal data in a structured commonly used and machine readable form to a third party (this right only applies in very limited circumstances);
- (j) object to direct marketing;
- (k) object to automated decision making.

The legislation requires that appropriate technical and organisational measures shall be taken to prevent accidental or unlawful disclosure of personal data.

All data and records will be stored as securely as possible in order to avoid potential misuse or loss.

Staff should be aware that, subject to certain exemptions, that –

It is a criminal offence to knowingly or recklessly without the consent of the data controller to disclose personal data or the information contained in personal data or to procure such disclosure to another person.

Data must not be disclosed to a third party unless the Data Protection Officer has given express written consent for you to do so.

Staff must never leave records unattended or in such circumstances where third parties may gain unauthorised access to them.

Paper records should be kept in the secure filing cabinets provided when not in use.

Computers should be "locked" when not in use.

Any contractors and temporary staff working for TWO Ltd. should sign non-disclosure agreements.

All requests for information received from clients and or data subjects should be handled with care and staff should ensure that the person requesting the information is entitled to receive it.

In cases of doubt or difficulty third party requests for details of personal data held by should be referred to the Data Protection Officer who will advise accordingly.

All subject access requests should be referred to the Data Protection Officer for advice.

Data retention

The length of time that personal data should be kept depends on the purpose for which it was obtained and the nature of the data. The periods for retaining records containing personal data are laid down either by statute or by good practice. Schedule 1 attached to this policy sets out the retention periods for the information that the company holds in respect of its staff, client staff and client data.

Destruction & disposal of personal data.

To ensure compliance with the GDPR/Data Protection Act all office paperwork containing personal data which has reached the end of the relevant retention period and is for disposal should be securely shredded.

Information held on digital media such as computer hard drives, CD-ROMs, DVD, Flash drives and the like should be destroyed in such a manner that information cannot be retrieved. Destruction of back-up copies of such data will also be dealt with in the same manner.

Policy on Retention, Security & Disposal of Personal Data

Schedule 1

Record	Retention Period	Reason
Client data submitted immigration advice and casework	Six years following the closure of the case	Statutory requirement of our regulator
Client staff personal data	Life of working relationship with client	Needed to maintain working relations.
TWO Ltd staff data	Two years beyond date of engagement	Statute and legal advice.
Disciplinary files	3 years after completion and appeal period expired	Legal advice.
Financial records	6 years	Statute.
Correspondence with clients	Life of working relationship with client plus six years	Needed to maintain working relations, plus statutory requirement of the regulator.
Version	Date	Comment
1.1	June 2021	GDPR version
2.0	June 2023	Review – minor grammatical amendments
3.0	June 2024	Annual review, no changes

