



DATA PROTECTION POLICY

TO MAKE *life* happy
FOR OUR *clients*
AND FOR *ourselves*




Our data protection policy sets out our commitment to protecting personal data and how we implement that commitment with regards to the collection and use of personal data.

We are committed to:

- ensuring that we comply with the eight data protection principles, as listed.
- meeting our legal obligations as laid down by the Data Protection Act 1998 and GDPR May 2018 and the resulting changes as listed.
- ensuring that data is collected and used fairly and lawfully
- processing personal data only in order to meet our operational needs or fulfil legal requirements
- taking steps to ensure that personal data is up to date and accurate
- establishing appropriate retention periods for personal data
- ensuring that data subjects' rights can be appropriately exercised
- providing adequate security measures to protect personal data
- ensuring that a nominated officer is responsible for data protection compliance and provides a point of contact for all data protection issues
- ensuring that all staff are made aware of good practice in data protection
- providing adequate training for all staff responsible for personal data
- ensuring that everyone handling personal data knows where to find further guidance
- ensuring that queries about data protection, internal and external to the organisation, is dealt with effectively and promptly
- regularly reviewing data protection procedures and guidelines within the organisation.

DATA PROTECTION PRINCIPLES

1. Personal data shall be processed fairly and lawfully.
2. Personal data shall be obtained for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act 1998.
7. Appropriate technical and organisational measures shall be taken against unauthorised and unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate



level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

GENERAL DATA PROTECTION REGULATION

GDPR is the regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU).

It also addresses the export of personal data outside the EU. The GDPR aims primarily to give control back to citizens and residents over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU.[1] When the GDPR takes effect, it will replace the data protection directive (officially Directive 95/46/EC)[2] of 1995.

The changes will apply to:

- lawful basis for processing
- consent and legitimate interest
- special category data
- criminal office data
- individual rights to be informed
- individual rights to access
- individual rights to rectification or erasure
- individual rights to data portability
- individual rights to object
- individual rights to restrict processing and automated decision making
- children
- exemptions