Data Protection Policy

Purpose of policy

Top2% is committed to all aspects of data protection and takes seriously its duties and the duties of its consultants, under the Data Protection Act 1998. This policy sets out how Top2% deals with personal data, including personnel information and data subject access requests, and consultants' obligations in relation to personal data.

This personal data may be used for a number of purposes, including without limitation, assessing the suitability of the consultant for assignments; providing details of the consultant to clients; dealing with requests and enquiries; maintaining records; assisting with police investigations and/or enquiries; and/or complying with statutory and regulatory obligations.

Data Protection Officer

Colum Price is the company data protection officer and is responsible for the implementation of this policy. If consultants have any questions about data protection in general, this policy or their obligations under it, they should direct them to ***Colum Price*** - contactable at colum.price@top2percent.co.uk.

Policy Statement

The Data Protection Act 1998 requires that eight data protection principles be followed in the handling of personal data. These principles require that personal data must:

- be fairly and lawfully processed;
- be processed for limited purposes and not in any manner incompatible with those purposes;
- be adequate, relevant and not excessive;
- be accurate;
- be kept no longer than is necessary;
- be processed in accordance with individuals' rights;
- be secure; and
- not be transferred to countries without adequate protection.

"Personal data"

The Data Protection Act 1998 applies only to information that constitutes "personal data". Information is "personal data" if it:

- identifies a person, whether by itself, or together with other information in the organisation's possession, or is likely to come into its possession; and

- is about a living person and affects that person's privacy (whether in his/her personal or family life, business or professional capacity), in the sense that the information has the person as its focus, or is otherwise biographical in nature.

Consequently, automated and computerised personal information about consultants held by Top2% is covered

by the Act. Personal information stored physically (for example, on paper) and held in any "relevant filing system" is also covered. In addition, information recorded with the intention that it will be stored in a relevant filing system, or held on computer, is covered.

A "relevant filing system" means a well-structured manual system that amounts to more than a bundle of documents about each employee filed in date order, e.g. a system to guide a searcher to where specific information about a named consultant can be located easily.

The use of personal information

The Data Protection Act 1998 applies to personal information that is "processed". This includes obtaining personal information, retaining and using it, allowing it to be accessed, disclosing it and, finally, disposing of it.

"Sensitive personal data"

"Sensitive personal data" is information about an individual's:

- racial or ethnic origin;
- political opinions;
- religious beliefs, or other beliefs of a similar nature;
- trade union membership (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992);
- physical or mental health or condition;
- sex life;
- commission or alleged commission of any criminal offence; and
- proceedings for any offence committed, or alleged to have been committed, the disposal of such proceedings, or the sentence of any court in such proceedings.

Top2% will not retain sensitive personal data without the express consent of the consultancy in question.

Top2% will process sensitive personal data, including injury records, in accordance with the eight data protection principles. If Top2% enters into discussions about a merger or acquisition with a third party, they will seek to protect consultant's data in accordance with the data protection principles.

General Data Protection Regulations (GDPR) Compliance

On the 25th May 2018, the Data Protection Regulations came into force. GDPR is concerned with respecting the rights of individuals when processing their personal information. This can be achieved by being open and honest with consultants, learners and personnel about the use of information about them and by following good data handling procedures. The regulation is mandatory and all organisations that hold or process personal data must comply.

The regulation contains 6 principles:

1) Personal data should be processed fairly, lawfully and in a transparent manner.
2) Data should be obtained for specified and lawful purposes and not further processed in a manner that is incompatible with those purposes.
3) The data should be adequate, relevant and not excessive.

4) The data should be accurate and where necessary, kept up to date.
5) Data should not be kept for longer than necessary.
6) Data should be kept secure.

All personnel have a responsibility to ensure that their activities comply with the data protection principles. The Director has responsibility for the type of personal data they collect and how they use it. Consultants should not disclose personal data outside the organisation's procedures, or use personal data held on others for their own purposes.

The Top2% Director, consultants and personnel are expected to comply with the new regulations summarised below and it should become embedded in the company's ethos during day-to-day data processing:

- Consultants and any personnel must agree to undergo GDPR training provided by the company, to ensure they understand the new regulations.
- All data, software and information stored on Top2% laptops, tablets, mobiles phones and other mobile devices, belong to Top2% and as such, may not be used for personal use.
- Hard copies of files, training records and/or documents which are being stored/archived, are still considered as being 'processed' under the terms of GDPR regulations and as such, are subject to the same rules.
- Hard copies of files, training records and/or documents, must be retained only for the length of time deemed necessary for legitimate purposes and where applicable, to meet legislative requirements in line with the Company's retention policy.
- Any company mobile devices (including mobile phones, tablets, computers), must contain sufficient security measures to prevent access by persons unauthorised to access it. This includes the use of strong, secure passwords and the use of the 'lock screen' function whilst the device is unsupervised, to prevent access to personal data by unauthorised persons.

By adhering to this policy, Top2% reduces its risk of liability against the following:

1) Using personal data for purposes other than those intended.
2) Unauthorised disclosure of personal data.
3) Unlawful use of special categories of data.
4) Using incorrect or out of date personal data.
5) Keeping data for longer than is necessary.
6) Being hacked.
7) Being phished.

Top2% commitment

Top2% will retain information about a consultants work history with Top2% and personal information, including address details and next of kin details.

Top2% will ensure that this personal information and any training records are securely retained. Any hard copies of information will be retained in a locked filing cabinet. Information stored electronically will be subject to access controls and passwords and encryption software will be used where necessary.

Should a consultant cease to work with Top2%, all of their electronic personal information will be deleted and hard copy documents confidentially shredded.

Data subject access requests

Top2% will inform each employee of:

- the types of information that it keeps about him/her;
- the purpose for which it is used.

Correction, updating and deletion of data

Consultants are entitled to check their personal information on a regular basis, so that they can correct, delete or update any data. If a consultant becomes aware that Top2% holds any inaccurate, irrelevant or out-of-date information about him/her, he/she must notify ***Colum Price*** immediately and provide any necessary corrections and/or updates to the information.

Data that is likely to cause substantial damage or distress

If a consultant believes that the processing of personal information about him/her is causing, or is likely to cause, substantial and unwarranted damage or distress to him/her or another person, he/she may notify Top2% in writing to the Director, to request Top2% put a stop to the processing of that information.

Within 21 days of receiving the employee's notice, Top2% will reply to the consultancy either:

a) that it has complied with, or intends to comply, with the request; or
b) the reasons why it regards the consultant's notice as unjustified to any extent and the extent, if any, to which it has already complied, or intends to comply, with the notice.

Consultant's obligations regarding personal information

If a consultant acquires any personal information in the course of his/her duties, he/she must ensure that:

a) the information is accurate and up to date, insofar as it is practicable to do so;
b) the use of the information is necessary for a relevant purpose and that it is not kept longer than necessary; and
c) the information is secure.

Where information is disposed of, consultants should ensure that it is destroyed. This may involve the permanent removal of the information from the server, so that it does not remain in a consultant's inbox or trash folder. Hard copies of information may need to be confidentially shredded. Consultants should be careful to ensure that information is not disposed of in a wastepaper basket/recycle bin.

If a consultant acquires any personal information in error by whatever means, he/she shall inform the Director immediately.

Where a consultant is required to disclose personal data to any other country, he/she must first ensure that there are adequate safeguards for the protection of data in the host country. For further guidance on the transfer of personal data outside the UK, please contact the Director**.**

If a consultant is in any doubt about what he/she may or may not do with personal information, he/she should

seek advice from the Director ***Colum Price***.

Consequences of non-compliance

All consultants are under an obligation to ensure that they have regard to the 6 data protection principles (see above) when accessing, using or disposing of personal information. Failure to observe the data protection principles within this policy may result in a consultant incurring personal criminal liability.

Monitoring and Review

Top2% may monitor consultant's performance through observation and client feedback. Top2% will inform the consultant that this monitoring is taking place and if any data is being collected, how the data will be securely processed and the purpose for which the data will be used. The consultant will usually be entitled to be given any data that has been collected about him/her. Top2% will not retain such data for any longer than is absolutely necessary.

Application of the policy

This policy, its principles and procedures, should be applied by the Director, consultants and other personnel who work in partnership with Top2%.

Top2% will provide an outline to all consultants on data protection matters on induction and where necessary thereafter. Top2% will review and ensure compliance with this policy at regular intervals.