DATA PROTECTION POLICY

Introduction

The business is required to comply with the law governing the management and storage of personal data, which is set out in the General Data Protection Regulation 2016 (GDPR).

For this reason, protection of personal data and respect for individual privacy is fundamental to the day-to-day operations of the business.

Compliance with the GDPR is overseen by the UK data protection regulator which is the Information Commissioner's Office (ICO). This business is accountable to the ICO for its data protection compliance.

Purpose

This policy aims to protect and promote the data protection rights of individuals and of the business, by informing everyone working for the business, of their data protection obligations and of the business procedures that must be followed in order to ensure compliance with the GDPR.

Scope

This policy applies to all staff (including managers), consultants and any third party that this policy has been communicated to.

This policy covers all personal data and special categories of personal data, processed on computers or stored in manual (paper based) files.

Responsibility

Nigel Willetts, who is the business's Data Protection Officer is responsible for monitoring the business's compliance with this policy.

Everyone in the business (and any third party to whom this policy applies to) is responsible for ensuring that they comply with this policy. Failure to do so may result in disciplinary action.

Data Protection Officer (DPO)

The business has appointed Nigel Willetts as its Data Protection Officer (DPO). Nigel Willetts's responsibilities within this role include:

- Developing and implementing data protection policies and procedures;
- Arranging periodic data protection training for all staff which is appropriate to their role;
- Acting as a point of contact for all colleagues on data protection matters;

- Monitoring the business's compliance with its data protection policy and procedures;
- Promoting a culture of data protection awareness;
- Assisting with investigations into data protection breaches and helping the business to learn from them;
- Advising on Data Protection Impact Assessments; and
- Liaising with the relevant supervisory authorities as necessary (i.e. the Information Commissioner's Office in the UK).

GDPR

The GDPR is designed to protect individuals and personal data which is held and processed about them by organisations or other individuals.

The GDPR uses some key terms to refer to individuals, those processing personal data about individuals and types of data covered by the Regulation. These key terms are:

Personal data Means any information relating to an identified and identifiable natural person ('data subject'). E.g. information from which a person can be identified, directly or indirectly, by reference to an identifier i.e. name; ID number; location data; online identifiers etc.

It also includes information that identified the physical, physiological, genetic, mental, economic, cultural or social identity of a person.

For the business's purposes, our clients are data subjects (other individual third parties that we hold personal data about are also likely to be data subjects).

Controller - Means the natural or legal person, public authority, agency or other body who alone or jointly with others, determines the purposes and means of processing the personal data. I.e. the controller is the individual, organisation or other body that decides how personal data will be collected and used.

For the business's purposes, this business is a data controller.

Processing - Means any operation which is performed on personal data such as: collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

For the business's purposes, everything that we do with client information (and personal information of third parties) is 'processing' as defined by the GDPR.

Special categories of personal data - Means personal data revealing:

a) racial or ethnic origin;
b) political opinions;
c) religious or philosophical beliefs;
d) trade-union membership;
e) the processing of genetic data or biometric data for the purpose of uniquely identifying a natural person;
f) data concerning health or data concerning a natural person's sex life or sexual orientation

N.B. data relating to criminal convictions and offences is not included within the special categories however there are additional provisions for processing this type of data (see Regulation 10 of GDPR)

Data Protection Principles

The GDPR is based around 8 principles which are the starting point to ensure compliance with the Regulation. Everybody working for the business must adhere to these principles in performing their day-to-day duties. The principles require the business to ensure that all personal data and sensitive personal data are:

(a) Processed lawfully, fairly and in a transparent manner in relation to the subject ('lawfulness, fairness and transparency')

(b) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ('purpose limitation')

(c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')

(d) Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy')

(e) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which personal data are processed ('storage limitation')

(f) Processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage using appropriate technical or organisational measures ('integrity and confidentiality')

The business must be able to demonstrate its compliance with (a) – (f) above ('accountability').
Processing personal data and sensitive personal data

The business must process all personal data in a manner that is compliant with the GDPR, in short, this means that it must.

- have legitimate grounds for collecting and using the personal data;
- not use the data in ways that have unjustified adverse effects on the individuals concerned;
- be transparent about how you intend to use the data, and give individuals appropriate privacy notices when collecting their personal data;
- handle people's personal data only in ways they would reasonably expect; and
- make sure you do not do anything unlawful with the data.

The business must ensure that you are aware of the difference between personal data and special categories of personal data and ensure that both types of data are processed in accordance with the GDPR.

The conditions for processing special categories of personal data that are most relevant to our business are:

- Explicit consent from the data subject;
- The processing is necessary for the purposes of carrying out the business's obligations in respect of employment and social security and social protection law;

7 The Lanterns, 16 Melbourn Street, Royston, Herts, SG8 7BX
Telephone: 0808 146 7000 Facsimile: 0800 019 1866 Email: sales@calteq.co.uk

- The processing is necessary to protect the vital interests of the data subject or another person;
- The processing relates to personal data that has already been made public by the data subject; or
- The processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.

If you have any concerns about processing personal data, please contact Nigel Willetts, who will be happy to discuss matters with you.

Rights of the data subject

The GDPR gives rights to individuals in respect of the personal data that organisations hold about them. Everybody working for the business must be familiar with these rights and adhere to the business's procedures to uphold these rights.

These rights include:

- Right of information and access to confirm details about the personal data that is being processed about them and to obtain a copy;
- Right to rectification of any inaccurate personal data;
- Right to erasure of personal data held about them (in certain circumstances);
- Right to restriction on the use of personal data held about them (in certain circumstances);
- Right to portability – right to receive data processed by automated means and have it transferred to another data controller;
- Right to object to the processing of their personal data.

If anybody receives a request from a data subject (a client or other third party that we hold personal data about) to exercise any of these rights, the request must be referred to Nigel Willetts the DPO, immediately or to Mike Stephenson, Company Director, in his absence.

Note: The business has one month to respond to a request to access a copy of personal data.

Confidentiality and data sharing

The business must ensure that it only shares personal information with other individuals or organisations where it is permitted to do so in accordance with data protection law.

Wherever, possible you should ensure that you have the client's (or other data subject's) consent before sharing their personal data. Although, it is accepted that this will not be possible in all circumstances, for example if the disclosure is required by law.

Any further questions around data sharing should be directed to Nigel Willetts, Data Protection Officer.

Data Protection Impact Assessments (DPIAs)

DPIAs are required to identify data protection risks; assess the impact of these risks; and determine appropriate action to prevent or mitigate the impact of these risks, when introducing, or making significant changes to, systems or projects involving the processing of personal data.

In simpler terms, this means thinking about whether an organisation is likely to breach the GDPR and what the consequences might be, if the organisation uses personal data in a particular way. It is also

about deciding whether there is anything that the organisation can do to stop or minimise the chances of potential problems identified, from happening.
DPIAs will be undertaken by management or designated project managers.

Breaches

A data protection breach is defined as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed".

Everybody working for the business has a duty to report any actual or suspected data protection breach without delay to their line manager and Nigel Willetts, Data Protection Officer.

Breaches will be reported to the Information Commissioner's Office (ICO) by Nigel Willetts, Data Protection Officer without undue delay and, where feasible, not later than 72 hours after having become aware of the breach. Unless, the business is able to demonstrate that the personal data breach is unlikely to result in a risk to the rights and freedoms of data subjects.

Nigel Willetts, Data Protection Officer will maintain a central register of the details of any data protection breaches.

Complaints

Complaints relating to breaches of the GDPR and/ or complaints that an individual's personal data is not being processed in line with the data protection principles should be referred to Nigel Willetts, Data Protection Officer without delay.

Penalties

It is important that everybody working for the business understands the implications for the business if we fail to meet our data protection obligations. Failure to comply could result in:

- Criminal and civil action;
- Fines and damages;
- Personal accountability and liability;
- Suspension/ withdrawal of the right to process personal data by the ICO;
- Loss of confidence in the integrity of the business's systems and procedures;
- Irreparable damage to the business's reputation.

Note: The business could be fined up to €20,000,000, or up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.