Private & Confidential

DATA PROTECTION POLICY

May 2018
Version 1

Contents

1 Purpose of the Policy

The Klesch Group ("Klesch") is committed to protecting the rights and privacy of individuals in line with the General Data Protection Regulation ("GDPR"). Klesch need to collect and use certain types of personal information in order to carry out their work. This information must be collected and dealt with appropriately. This Data Protection Policy ("the Policy") has been formulated to support this commitment.

The GDPR governs the use of "Personal Data". Personal Data is defined in the GDPR as any information relating to an identified or identifiable natural person ("Data Subject") who can be identified directly or indirectly. Personal Data can be held on computers, laptops and mobile devices, or in a manual file and includes email, minutes of meetings and photographs.

Klesch will remain the data controller for all Personal Data held. All employees and consultants employed by Klesch will be personally responsible for processing and using personal information in accordance with this Policy.

This Policy has been approved by the Chairman of the Klesch Group and will remain in force until further notice. It will be amended, updated and added to on an ongoing basis as and when required.

In the event that there is a conflict between the business unit's policy and this Policy, this Policy will take precedence.

2 Applicability of the Policy

This Policy applies to all

- Employees of Klesch,
- Independent contractors, agents, and consultants that may be employed/engaged by Klesch for a specific project or duration.

3 Principles and Law of GDPR

Klesch endorses fully and adheres to the six principles of data protection, as set out in the Article 5 of the GDPR. These principles apply regardless of whether data is stored electronically, on paper or on other materials. Personal Data must be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, are erased or rectified without delay.
- Kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the personal data are processed.
- Processed 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.

These principles must be followed at all times when processing or using personal information. Therefore, through appropriate management and strict application of criteria and controls, Klesch will:

- Observe fully the conditions regarding the fair collection and use of information including the giving of consent
- Meet its legal obligations to specify the purposes for which information is used
- Collect and process appropriate information only to the extent that it is needed to fulfil our operational needs or to comply with any legal requirements
- Ensure the quality of information used
- Ensure that the information is held for no longer than is necessary
- Ensure that the rights of people about whom information is held can be fully exercised under the GDPR (i.e. the right to be informed that processing is being undertaken, to access one's personal information; to prevent processing in certain circumstances, and to correct, rectify, block or erase information that is regarded as incorrect)
- Take appropriate technical and organisational security measures to safeguard personal information
- Publicise and abide by individuals' right to appeal or complain to the supervisory authority (the Information Commissioner's Office (ICO)) in the event that agreement cannot be reached in a dispute regarding data protection
- Ensure that personal information is not transferred abroad without suitable safeguards.

4 Designated Data Controllers

The Designated Data Controllers for Klesch are Tom Baxter & Jennifer Wyatt. Anyone requiring guidance and assistance in implementing this Policy or who considers that the Policy has not been followed in any way should raise the matter with one of these Data Controllers.

5 Staff Responsibilities

All employees of Klesch including contractors and volunteers are responsible for:

- Reading and complying with this Policy.
- Checking that any information they provide to Klesch in connection with their employment is accurate and up to date
- Informing Klesch of any changes to information that they have previously provided, e.g. changes of address. Klesch cannot be held responsible for any errors unless the relevant employee has informed it of such changes.

6 Data Security

All employees of Klesch including contractors and volunteers are responsible for ensuring that:

- Any Personal Data that they hold is kept securely
- Personal Data is not disclosed either orally or in writing or via Web pages or by any other means, accidentally or otherwise, to any unauthorised third party.

Employees should note that unauthorised disclosure of Personal Data will usually be a disciplinary matter and may be considered gross misconduct in some cases. Personal information should be kept in a locked filing cabinet, drawer, or safe. If it is computerised, it should be coded, encrypted or password protected both on a local hard drive and on a network drive that is regularly backed up. If a copy is kept on removable storage media, that media must itself be kept in a locked filing cabinet, drawer, or safe.

7 Disaster Recovery

Klesch backs up data every day and has multiple copies (at least one set for each day of the week and additional weekly ones in order to have at least a month's worth of data at any one time). Records are secured by:

- Backups are kept off site on cloud.
- Backups are verified regularly by the software and system supplier.
- Firewalls and virus checkers which are kept up to date and running, and users are trained in virus avoidance and detection.
- Computers which are protected from physical harm, theft or damage, and from electrical surges using protective plugs.
- Klesch plans for how to deal with loss of electricity, external data links, server failure, and network problems. It uses paper forms where necessary for temporary record keeping.

8 Subject Consent

The GDPR sets a high standard for consent and requires a positive opt-in. Neither pre-ticked boxes nor any other method of default consent are allowed. As required by the GDPR, Klesch takes a "granular" approach i.e. it asks for separate consent for separate items and will not use vague or blanket requests for consent. As well as keeping evidence of any consent, Klesch ensures that people can easily withdraw consent (and will guide them on how this can be done).

It should be noted, however, that consent is only one of the lawful bases on which data processing depends. Others include the following:

- Contract: if processing someone's personal data it is necessary to fulfil Klesch's contractual obligations to them (e.g. to pay their salary).
- Legal obligation: if processing personal data it is necessary to comply with a common law or statutory obligation.
- Vital interests: to protect someone's life (and even then, it cannot be relied on with regard to health data or other special category data if the individual is capable of giving consent.
- Legitimate interests: when data is used in ways people would reasonably expect and which have a minimal privacy impact, or where there is a compelling justification for the processing.

9 Subject Access

An employee may request details of personal information which Klesch holds about them under the GDPR. If an employee would like a copy of the information held on them, they should write to HR. The requested information will be provided within four weeks. If there is any reason for delay, that will be

communicated within the four week time period. A request which is manifestly unfounded or excessive may be refused. The person concerned will then be informed of their right to contest this decision with the supervisory authority (the ICO).

If an employee believes that any information held on them is incorrect or incomplete, then they should contact HR as soon as possible and they will promptly correct any information found to be incorrect.

10 Disclosing Data for other Reasons

In certain circumstances, the GDPR allows personal data to be disclosed to law enforcement agencies without the consent of the Data Subject.

Under these circumstances the Data Controller will ensure the request is legitimate, and after seeking advice from Klesch management and from Klesch's legal advisors where necessary, respond to any such legitimate request.

11 Breach of Policy

In the event that this Policy is breached, Klesch HR will immediately assess the magnitude of the breach and will follow the process as outlined below:

The relevant Klesch business unit will provide a summary of the reason for the breach of the Policy and any financial impact to Group Risk.

Klesch HR will then report the breach to the Klesch Group Chairman and recommend any necessary actions, which may include disciplinary action up to and including summary dismissal.