DATA PROTECTION POLICY

General Statement of the Company's Duties and Scope

The Company is required to process relevant personal data regarding members of staff, sub-contractors, applicants and customers as part of its operation and shall take all reasonable steps to do so in accordance with this Policy.

Data Protection Controller

The Company has appointed the CEO as the Data Protection Controller (DPC) who will endeavour to ensure that all personal data is processed in compliance with the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) adopted 27 April 2016, the two-year transition period and the application date of 25 May 2018.

The Principles

The Company shall so far as is reasonably practicable comply with the Data Protection Principles (the Principles) contained in the Data Protection Act to ensure all data is:

- Fairly and lawfully processed
- Processed for a lawful purpose
- Adequate, relevant and not excessive
- Accurate and up to date
- Not kept for longer than necessary
- Processed in accordance with the data subject's rights
- Secure
- Not transferred to other countries without adequate protection

Data Protection Policy

Definitions

- The Company is the *O3C Konsult AB* group, including Direct Validation and similar services.
- Data Subject, an individual who is the subject of the personal data.

Personal Data

Personal data covers both facts and opinions about an individual where that data identifies an individual. For example, it includes information necessary for employment such as the member of staff’s name and address and details for payment of salary.

Sensitive data

No sensitive personal data as defined in the GDPR is stored.

Processing of Personal Data

Consent may be required for the processing of personal data unless processing is necessary for the performance of the contract of employment. Any information which falls under the definition of personal data and is not otherwise exempt will remain confidential and will only be disclosed to third parties with appropriate consent.

The Company processes some personal data for marketing and sales, data subjects have the right to request an opt-out to these activities, which must be respected.

Rights of Access to Information

Data subjects have the right of access to information held by the Company, subject to the provisions of the GDPR. The Company will endeavour to respond to any such written requests as soon as is reasonably practicable and in any event within 30 days.

Exemptions

Certain data is exempted from the provisions of the Data Protection Act which includes the following:-

• National security and the prevention or detection of crime

• The assessment of any tax or duty

• Where the processing is necessary to exercise a right or obligation conferred or imposed by law upon the Company, including Safeguarding and prevention of terrorism and radicalisation

• Information falling under the Client-Attorney privilege.

The above are examples only of some of the exemptions under the Act. Any further information on exemptions should be sought from the DPC.

Accuracy

The Company will endeavour to ensure that all personal data held in relation to all data subjects is accurate. Data subjects must notify the data processor of any changes to information held about them. Data subjects have the right in some circumstances to request that inaccurate information about them is erased. This does not apply in all cases, for example, where records of mistakes or corrections are kept, or records which must be kept in the interests of all parties to which they apply.

Enforcement

If an individual believes that the Company has not complied with this Policy or acted otherwise than in accordance with the GDPR, the member of staff should utilise the DPC.

Data Security

The Company will take appropriate technical and organisational steps to ensure the security of personal data.

All staff will be made aware of this policy and their duties under the policy.

The Company and therefore all staff are required to respect the personal data and privacy of others and must ensure that appropriate protection and security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to all personal data.

An appropriate level of data security must be deployed for the type of data and the data processing being performed. In most cases, personal data must be stored in appropriate systems and be encrypted when transported offsite. Other personal data may be for publication or limited publication within the Company, therefore having a lower requirement for data security.

External Processors

The Company must ensure that data processed by external processors, for example, service providers, Cloud services including storage, web sites etc. are compliant with this policy and the relevant legislation.

Secure Destruction

When data held in accordance with this policy is destroyed, it must be destroyed securely in accordance with best practice at the time of destruction.

Retention of Data

The Company may retain data for differing periods of time for different purposes as required by statute or best practices. Other statutory obligations, legal processes and enquiries may also necessitate the retention of certain data.

The Company may store some data such immaterial right information up to 10 year after the expiry of the rights.

Author: CEO

Date: Spring 2018