General Data Protection Regulations - GDPR

DATA CLEANSING POLICY

1. INTRODUCTION

1.1 Data subjects have certain rights in respect of their personal data. When we process data subjects' personal data, we shall respect those rights. This policy provides a framework for dealing with data cleansing. It is our policy to ensure that data retention and cleansing in respect of personal data is handled in accordance with applicable law.

1.2 This policy outlines what action we will take and within what time frames in relation to the retention and cleansing of personal data, to ensure we are compliant with data protection law (in particular the GDPR) and best practice.

2. DEFINITIONS

2.1 For the purposes of this policy, the following terms have the following meanings:

Data: is information which is stored electronically, or in certain paper-based filing systems.

Data subjects: means all living individuals about whom we hold personal information

Personal data: means any information relating to an identified or identifiable data subject. An identifiable data subject is anyone who can be identified, directly or indirectly, by reference to an identifier, such as a name, identification number or online identifier.

DPO: Data Protection Officer

GDPR: the General Data Protection Regulations

ICO: the Information Commissioner's Office

Processing: is any operation or set of operations that is performed on personal data, such as collection, use, storage, dissemination and destruction.

3. RESPONSIBILITIES OF THE DPO OR PERSON WITH RESPONSIBILITY FOR THE OPERATION OF THIS POLICY

3.1 The DPO or person with responsibility for the operation of this policy ("the Responsible Officer") shall be responsible for ensuring that all personal data kept by the business, whether for current or archive purposes, is kept securely and with due regard to best current practice in terms of IT and physical security, and to guard so far as is possible against unauthorised access to such data.

3.2 In furtherance of 3.1 above the Responsible Officer shall undertake regular reviews, and in any event at 12 monthly intervals, of the security of the storage of all data records including without limitation their location and accessibility both internally and externally.

3.3 The Responsible Officer shall be responsible for regular and timely reviews of personal data records, and in any event at 12 monthly intervals, to evaluate whether and to what extent such data can be safely and securely deleted in accordance with the following time scales. Data cleansing shall be considered under the following categories:

3.3.1 Financial data shall be retained for seven years;

3.3.2 Marketing data where such data does not relate to a current client of the business shall be retained for two years following the most recent engagement with the client or prospect. For these purposes engagement shall mean some activity that denotes a willingness on the part of the data subject to continue to receive marketing communications for example,

specific opt in, continuing to open and engage with email messages where the business is able to track such action, contacting the business to enter or continue with discussions relating to possible future business dealings. Where the business is not relying on documented consent to the sending of marketing materials, this policy does not override the responsibility of the Responsible Officer to ensure that the appropriate Legitimate Interest Assessment ("LIA") has been conducted in relation to this category of data processing, that the LIA supports the decision that an active opt in is not needed and that the appropriate Legitimate Interest has been communicated to the client or prospect whether in the business's privacy policy or otherwise.

3.3.3 Potential employee data where such individual does not become an employee of the business shall be retained for one year from the date of last contact with the individual;

3.3.4 Employee data shall be kept for seven years. Thereafter such data shall be minimised so that what is retained includes only the following: name; address; dates of employment; roles in which employed; main place(s) of work.

3.3.5 Client and supplier data shall be kept indefinitely so that the business can protect its Legitimate Interests in the event of future legal action. The business shall conduct and keep under review such LIA's as shall be necessary to retain this category of personal data.

4 Deletion of Personal Data

4.1 No personal data shall be deleted except on the authority of the Responsible Officer, who shall keep appropriate records of the deletion of such data.

4.2 All data shall be deleted securely and with due regard to best practice at the time the deletion takes place.