CLICK4GROUP GDPR Disposal Policy

Who We Are (The Company)

Click4Group.co.uk, Click4Warranty.co.uk and Click4Gap.co.uk are all trading styles of Future 45 Limited (The Company)

ADDRESS..... Trident Court, 1 Oakcroft Road, Surrey, KT9 1BD
COMPANY REGISTRATION No..... 5407413
DATA PROTECTION REGISTER No. Z933878X
FINANCIAL CONDUCT AUTHORITY (FCA) No..... 461102
0208 819 3424
email@click4group.co.uk

Purpose Of This Policy

The purpose of this policy is to detail the procedures for the disposal of information to ensure that we carry this out consistently and where required we fully document any actions taken. Unless otherwise specified the disposal policy refers to both hard and soft copy documents.

Destruction of Data

The Company and its employees should, on a regular basis, review all data, whether held electronically or on paper, to decide whether to destroy or delete any data once the purpose for which those documents were created is no longer relevant. See CLICK4GROUP GDPR Data Retention Policy "Lawful Retention Periods" for the retention schedule. Overall responsibility for the destruction of data falls to the Data Protection Officer.

Once the decision is made to dispose according to the CLICK4GROUP GDPR Data Retention Policy, the data should be deleted, shredded or otherwise destroyed to a degree equivalent to their value to others and their level of confidentiality. The method of disposal varies and is dependent upon the nature of the document. For example, any documents that contain sensitive or confidential information (and particularly sensitive personal data) must be disposed of as confidential waste and be subject to secure electronic deletion; some expired or superseded contracts may only warrant in-house shredding.

In this context, the employee shall perform the tasks and assume the responsibilities relevant for the information destruction in an appropriate way. The specific deletion or destruction process may be carried out either by an employee or by an internal or external service provider that the Data Protection Officer subcontracts for this purpose. Any applicable general provisions under relevant data protection laws and the Company's Personal Data Protection Policy shall be complied with.

Appropriate controls shall be in place that prevents the permanent loss of essential information of the company as a result of malicious or unintentional destruction of information – these controls are described in the company's Information Security Policy.

The Data Protection Officer shall fully document and approve the destruction process. The applicable statutory requirements for the destruction of information, particularly requirements under applicable data protection laws, shall be fully observed.

Document Disposal Methods

Documents containing information that is of the highest security and confidentiality and those that include any personal data shall be disposed of as confidential waste (cross-cut shredded and incinerated) and shall be subject to secure electronic deletion. Disposal of the documents should include proof of destruction.

Documents that contain confidential information such as parties' names, signatures and addresses, or which could be used by third parties to commit fraud, but which do not contain any personal data should be cross-cut shredded and collected by an approved disposal firm, and electronic documents will be subject to secure electronic deletion.

Documents that do not contain any confidential information or personal data and are published Company documents should be strip-shredded or disposed of through a recycling company and include, among other things, advertisements, catalogues, flyers, and newsletters. These may be disposed of without an audit trail.

More Information

If you're looking for more information, please let us know by contacting our Data Protection officer by telephone, email or post. All contact details are available at the top of this document.