United Business Group Limited

DATA Protection Policy

January 2021: Version UBG LTD

The 'Data Controller' is the Company. The Data Protection Officer within United Business Group Limited is Terry Woods. He is responsible for Data Protection within the Company and for maintenance of the 'Policy'. The day to day implementation of the 'Policy' is delegated to, Colin Cornhill.

Purpose and Compliance of this Policy

The purpose of this Policy is to comply with the law, follow good practice, protect clients, staff, and other individuals, and protect the Company. All members of staff, whether permanent or temporary, have a duty to abide by the Data Protection Act 1998 (Data Protection (Amendment) Act 2018 - "DPA"

In order to comply with the **Requirements** and **Client Awareness,** this Policy applies to:

- (i.e.) the UK office of United Business Group Limited
- Its branches and regions;
- All paid staff (including temporary contract Staff);
- All sessional workers operating on behalf of United Business Group Limited

This paper details the policy.

All staff should be aware of the need for the preservation of utmost confidentiality of any information acquired by members of the Company regarding clients, potential clients, or records kept. Such confidentiality also applies to any other dealings or processes within the Company. Data / information should only be given to those who have a right to that information. (*See 7.*)

All staff are required to read, understand, and accept any policies and procedures that relate to the personal data they may handle in the course of their work.

1 The requirement - Data Protection Principles

Anyone processing personal data must comply with the eight enforceable principles of good practice. They are that data must be:

- fairly and lawfully processed;
- processed for limited purposes;
- adequate, relevant, and not excessive;
- accurate and up to date;
- not kept longer than necessary;
- processed in accordance with the data subject's rights;
- secure;
- not transferred to countries without adequate protection.

2 Personal Data

"Personal data" can be defined as information about living, identifiable individuals, covering both facts and opinions about the individual, but need not be sensitive information. It can be as little as name and address but must be processed in accordance with the Data Subject's rights. Such data can either be automated (i.e. part of a computer record) or manual record.

3 Policy Statement

United Business Group Limited will:

- comply with both the law and good practice;
- respect individuals' rights;
- be open and transparent with individuals whose data is held;
- provide training and support for staff (including temporary contract staff) who handle personal data
- keep information securely;

- hold good quality information

- give individuals as much choice as possible and reasonable over what data is held and how it is used

4 Key Risks

The Data Controller has identified the following potential key risks, which this Policy is designed to address:

- Breach of confidentiality (information being given out inappropriately),
- Insufficient clarity about the range of uses to which data will be put,
- Failure to offer choice about data use when appropriate,
- Breach of security by allowing unauthorised access,
- Failure to establish efficient systems of managing changes leading to personal data not being accurate and up to date,
- Harm to individuals if personal data is not kept up to date
- Data Processor contracts

5 Client Awareness

Clients should be made aware of the identity of the Data Controller, any uses to which personal data will be put and any proposed disclosure of data to third parties. This must be done at the time the customer first provides the personal data. Data must be fairly and lawfully processed and processing may only be carried out where the following conditions have been satisfied:

- the processing complies with both law and good practice;
- the individual has given his/her consent to the processing (this will always be a requirement of the client firm when sensitive personal data, such as details of the individual's physical condition, is provided);
- the processing is necessary to protect the vital interests of the individual;
- the processing is necessary in order to pursue the legitimate interests of the Data Controller or certain third parties (unless prejudicial to the interests of the individual).

6 Provision of Client data

Client Data may only be given to:

- the client
- other relevant members of staff;
- offices with whom the clients business is being placed – and only the necessary data to be able to place that business;
- the Regulators, e.g. the FCA, of the particular type of business, subject to prior authority from the Data Control Manager (Data Protection Officer);
- our Compliance Consultants, who are currently Thistle Initiatives Limited subject to prior authority from the Data Control Manager.

When giving information to a client, particularly by telephone, it is most important that the client's identity is verified. If in doubt, questions should be asked of the client, to which only he/she is likely to know the answers. **Do not give information to other parties, even if related.** i.e. you must not give details of a wife's insurance or investment contracts to the husband, without the express permission of the client (the wife).

7 Subject Access Requests ("SARs")

Clients are entitled under the DPA to ask for information held by us about them. SARs must be made in writing and addressed to the Data Control Manager (Data Protection Officer). All staff (including temporary contractors) are required to pass on anything which might be a SAR immediately to the Data Control Manager (Data Protection Officer). Where the individual making a SAR is not known personally to either the Data Control Manager (Data Protection Officer) or member of staff supplying such data, their identity will be required to be verified before providing such information. Need to confirm with Client who actually deals with SARs within the Company. This is usually the Data Protection Officer but if individual staff members dealing, will need to add the following:

Should the client/data subject ask to see his or her full records, he/she should be asked to be specific, in relation to a particular piece of business. Any request should be referred to the Data Protection Officer. This must be done immediately as requests are subject to a strict timetable. If the Data Protection Officer is not available, some other

senior person within the Company must be informed. In providing the requested data, the confidentiality of other client's records is paramount and therefore must not be compromised.

When a SAR is received, it must be dealt with promptly and in any case, within 40 days. We may make a charge of up to £10 [up to £50 where medical data is involved]. When providing the information, we will also provide a description of why the information is processed, to whom it has been disclosed and the source of the data. If making a charge, the 40 days does not start until the money is received. The requested information will be provided in permanent form unless the applicant makes a specific request to be given supervised access in person.

Reference should be made to the guidance on SARs issued by the ICO on 8th August 2013 and available on the ICO website at http://www.ico.org.uk/news/latest_news/2013/New-ICO-Subject-Access-Code-of-Practice

8 Client Consent

(*This section may not apply to all clients if consent is not included in a contract/client service agreement. The client may therefore wish to alter some of these points. E.g. he/she may wish to nominate a person to whom information may be given. If so, the alteration should be written in and signed by the client*).

Apart from initial contact information, Client Data will not be kept without the express permission of the client. This permission is given in most, but not all, circumstances by the signature of the client at the foot of a section in the Client Contract/Client Service Agreement, which states:

> In order to advise you properly, we must obtain certain information from you about your financial and personal circumstances, to assess your suitability for particular products and services. We will also need to maintain certain other records:
>
> 1) You agree that the information we hold about you can be held on computer and/or paper files.
> 2) You agree that any information we hold about you may be disclosed:
> a. to third parties (e.g. credit agencies and product providers) for the purpose of processing your application;
> b. the Regulators (mainly the Financial Conduct Authority who have a legal authority to check all our records);
> c. our Compliance consultants, who help to ensure that, in your interests, we abide by the Financial Services Act and other regulations; but,
> d. must not be disclosed to any other parties (even if related) without your express permission in writing.
>
> 3) You agree that we may use the information that we hold about you to contact you from time to time by post, fax, e-mail, or telephone to bring to your attention products, services or information about your existing contracts which may be of benefit to you. You may opt out of this condition by putting an X in the following box. ☐
> 4) You understand that we have a legal obligation to ensure that the information within our records is kept up to date, but can only do so if provided with the up to date information by you.
> 5) You understand that you may withdraw the consent given by you to the above paragraphs 2) d. and 3) at any time by informing us in writing.

9 "Suppression List"

A list must be kept of clients who have asked not to be sent marketing material. Maintenance of this list is the responsibility of the Data Control Manager (Data Protection Officer), to whom client requests should be given. Should we at any time make use of a mailing list, it should be checked against the "suppression list".

10 Confidentiality

As confidentiality applies to a much broader range of information than Data Protection, A Confidentiality Policy may also be implemented, all confidential information is indicated within United Business Group within a Red Folder structure and is locked away in metal filing cabinets.

11 Staff Training & Acceptance of Responsibilities

All members of staff should be constantly aware of the possibility of confidential Data being seen by unauthorised personnel - such as visible access to computer screens by the general public, visiting clientele and other visitors, to the Company as well as leaving confidential client details on desks overnight. Such information should be kept in a locked cupboard when not in use.

The use of computer passwords is a requirement of the Company to avoid unauthorised access. All staff have unlimited access to client records in order to perform their tasks. Cloud Back up is schedules daily by Acromus and managed by our IT department

No information should be put on the computer from outside sources, such as mailing lists, without the express authority of the Data Protection Officer.

12 Accuracy of Personal Data

The Company will review personal data regularly to ensure that it is accurate, complete, and up to date. However, all members of staff must be constantly aware of the need to abide by the Data Protection Principles, as noted in paragraph 1 above. Data held shall be adequate, relevant, and not excessive in relation to the purpose or purposes for which they have been collected or are further processed and shall not be kept for longer than is necessary for that purpose or purposes. Out of date information should therefore be discarded if no longer relevant or required, or a line put through it if out of date but needed to support other evidence. Fact finds should be updated at each meeting with the client and reference made on both the new fact find information sheet and previous one. In reality most relevant information should be kept for the life of the contract or the association with the client, PLUS a period of years as required by the Regulator.

13 Recording of Data

Information and records relating to clients will be stored securely, within the guidelines of the Information Commissioner and will only be assessable to authorised staff. Information will be stored only for as long as needed or required by statute and will be disposed of appropriately. In reality most relevant information should be kept for the life of the contract or the association with the client, PLUS a period of years as required by the Regulator.

However, such data may be inspected by the Ombudsman, the Courts or some legal official.

Records should be kept in such a way that the recorder (Adviser or support staff) would be happy for the client to inspect them. It should also be born in mind that at some time in the future the Data may be inspected by the Ombudsman, the Courts or some legal official. It should therefore be accurate, unbiased, unambiguous, clearly decipherable / readable, and up to date.

14 Transfer of Data Outside the EU

If data is to be transferred outside of the EEA the specific consent of the data subject concerned must be obtained before the transfer takes place OR the transfer is permitted if the non-EEA country to which the data is being transferred has equivalent data protection legislation.

The European Economic Area means the 27 EU member states plus Norway, Iceland, and Liechtenstein. Currently only Switzerland, Israel, Canada, and Argentina are recognised as countries having adequate protection. In addition companies registered under the Safe Harbour regime in the USA are also recognised.

Consent from data subjects can be obtained by the customer including relevant information in its privacy policy and ensuring that its clients actively consent to transfers of their data outside of the EEA when they register to use the customer's products or services. Any transfer of data to any other country or without the data subject's consent will be illegal.

15 Staff Training & Acceptance of Responsibilities

All staff (permanent or temporary) will have their responsibilities outlined during their induction procedures. Training will be given to all staff. Members of staff should also read the additional material provided in this section of the Staff Handbook.

16 Discipline

This policy has been approved by the Directors and any breach will be taken seriously and may result in formal action. Therefore, noncompliance by staff is considered a disciplinary matter which, depending upon the circumstances, could lead to dismissal. **It should be noted that an individual can commit a criminal offence under the Act, for example by obtaining and / or disclosing personal data for his/her own purposes without the consent of the Data Controller.** Noncompliance with the requirements of the Data Protection Act by a member of staff could also lead to serious action being taken by third parties against the Company.

Any employee who considers that the policy has not been followed in respect of personal data about themselves should raise the matter with their Line Manager or the Company's Information Compliance Manager in the first instance.

17 What to do if a breach occurs

A data security breach can happen for a number of reasons:

- Loss or theft of data or equipment on which data is stored;
- Inappropriate access controls allowing unauthorised use;
- Equipment failure;
- Human error;
- Unforeseen circumstances such as a fire or flood;
- Hacking attack;
- 'Blagging' offences where information is obtained by deceiving the organisation who holds it;

But what should you do if you think a breach may have happened? ICO has published 'Guidance on data security breach management' at:

18 Data Protection and the FCA

The FCA considers Data Protection important. To help small firms manage their security it has provided guidance, which can be found on FCA web site https://www.fca.org.uk/

19 Related Policies / DP Clauses

- Confidentiality Policy
- Privacy Policy
- International Transfers of Personal Data – Clause

Signed:

Date:

Data Protection Officer

Further information:

The Information Commissioner can be contacted at:

Address:	Office of the Information Commissioner Wycliffe House Water Lane Wilmslow Cheshire, SK9 5AF
Telephone:	01625 545 700
Fax:	01625 524 510
Web:	www.dataprotection.gov.uk