DATA PROTECTION POLICY

Contents

1 Policy Statement

1.1 Everyone has rights with regard to how their personal data is handled. Personal data is any information that a person can be identified from and which is about that person, such as a name, address, account number, email address, location, CV or medical information.

1.2 During the course of our activities, UCFS Europe Company (**UCFS**) will collect, store and process personal data about our customers, suppliers, and other individuals with whom we communicate. This may include personal data we receive directly from those individuals (for example, where a customer applies for any of our products and/or services), data we gather ourselves (for example, through tracking online identifiers), or data we receive from other sources (including, for example, credit reference agencies, business partners, service providers and others).

1.3 Personal data, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the General Data Protection Regulation EU 2016/679, as well as other data protection and privacy laws such as the Privacy and Electronic Communications (EC Directive) Regulations 2003 and separate UK data protection law as may be updated or replaced from time to time (the **Data Protection Laws**). The enforcement of Data Protection Laws in the UK is regulated by the Information Commissioner's Office (the **ICO**) - you can find out more at www.ico.org.uk.

1.4 We recognise that the fair, transparent and lawful treatment of this data will maintain confidence in our organisation. This policy sets out our rules on data protection and the legal requirements that must be satisfied by UCFS and our employees in relation to the obtaining, handling, use, storage, transfer and destruction and other processing of such personal data.

1.5 This policy applies to all Data Users (as defined below). All Data Users should familiarise themselves with this policy and comply with its terms when processing personal data on behalf of UCFS in the course of their employment.

1.6 This policy does not form part of any employee's contract of employment and may be amended by us at any time.

2 Definition of Data Protection Terms

2.1 **Data subjects**, for the purpose of this policy, include all living individuals about whom we hold personal data.

2.2 **Personal data** means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

2.3 **Data controller** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. We are the data controller of all personal data used in our business for our own commercial purposes.

2.4 **Data Users** are those of our employees (including temporary employees, agency workers, contractors, interns and volunteers) whose work involves processing personal data. Data Users must protect the data they handle in accordance with this data protection policy and any applicable data security procedures at all times.

2.5 **Data processor** means a natural or legal person, public authority, agency or other body which processes personal data on our behalf and on our instructions, and which is not a data user.

2.6 **Processing** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

2.7 **Sensitive (special category) personal data** is a special category of personal data, including information about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health, sex life or sexual orientation, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Sensitive (special category) personal data can only be processed under strict conditions, including a condition requiring the express permission of the person concerned.

3 Data Protection Officer

3.1 The Data Protection Officer is responsible for ensuring our compliance with the Data Protection Laws and with this policy. The UCFS Data Protection Officer can be contacted by email at dpo@ucfs.net. If you have any questions or concerns about the operation of this policy, please contact the Data Protection Officer.

4 Data Protection Principles

All Data Users who process personal data under this policy must comply (and be able to demonstrate compliance) with the principles of the Data Protection Laws. These principles provide that personal data must be:

(a) be used in a way that makes it clear to data subjects what is being done with their personal data, and is fair, reasonable and compliant with Data Protection Laws;

(b) only be used in line with how we told the data subject we would use it and not for any wider, incompatible purposes;

(c) adequate, relevant and limited just to what we need it for;

(d) accurate and, where necessary, kept up to date;

(e) not kept in a form which permits identification of data subjects for any longer than necessary for the purpose for which the personal data is processed; and

(f) kept secure.

5 Fair and Lawful Processing

5.1 We must generally only process personal data (e.g. use, store, share, transfer or copy it) if one of the lawful bases set out in the Data Protection Laws applies.

5.2 This means that UCFS will only process personal data if one of the following applies:

(a) the data subject has given us their consent (we must ensure that the consent wording and mechanism for obtaining consent meet the requirements of the Data Protection Laws);

(b) we need to process the personal data to perform a contract with the data subject, or because they have asked us to take certain steps before entering into a contract (for example, we may require contact details so we can process certain requests);

(c) the processing is necessary to comply with a legal obligation to which we are subject;

(d) the processing is necessary to the protect someone's life or other vital interests;

(e) the processing is necessary to perform a task in the public interest; or

(f) the processing is necessary for UCFS's legitimate interest or the legitimate interests of a third party unless there is a good reason to protect the data subject's personal data which overrides those interests.

5.3 When sensitive (special category) personal data is being processed, additional conditions must be met, including receiving explicit consent from the data subject, and we shall ensure that such conditions are met when we are processing personal data as data controllers in the course of our business.

6 Special Category Personal Data and Background Checks

6.1 Some of the information we hold as a business is particularly sensitive and we must be aware that special rules apply to it.

6.2 UCFS will collect and use special category personal data in a number of circumstances, for example, for equal opportunities monitoring and where we are required to conduct criminal background checks as part of our recruitment processes.

6.3 The Data Protection Officer is responsible for monitoring UCFS's use of special category personal data. Data Users should consult with the Data Protection Officer when using special category personal data to ensure the correct compliance steps are taken.

7 Processing for Limited Purposes

7.1 Personal data may only be processed for the specific purposes notified to the data subject when the data was first collected or for any other purposes specifically permitted by law.

7.2 This means, broadly, that personal data must not be collected for one purpose and then used for another without the data subject being informed that their personal data will be used for a new purpose. If it becomes necessary to change the purpose for which personal data is processed, steps will need to be taken to inform the data subject of the new purpose before any processing occurs.

8 Notifying Data Subjects

8.1 To satisfy the transparency requirements under the Data Protection Laws, when collecting personal data directly from data subjects, UCFS needs to ensure that the data subjects receive fair information about how UCFS will use their data.

8.2 UCFS will provide them with the following information:

(a) our name and the contact details of the Data Protection Officer;

(b) the types of personal data which we are collecting and processing;

(c) why UCFS is processing their personal data and the lawful basis that applies (for example, consent or legitimate interests);

(d) if UCFS is processing the personal data on the basis of our or a third party's legitimate interests, UCFS must explain what those interests are;

(e) anyone with whom UCFS will share the personal data (either their name or a general description of them) – this includes any suppliers to whom UCFS may pass the data;

(f) details of transfers of the data outside the EU and safeguards UCFS have put in place (for example, entering into EU model contractual clauses);

(g) how long UCFS plan to retain the personal data or the criteria used to determine the retention period;

(h) their legal rights as data subjects (see paragraph 12 below);

(i) where we are processing on the basis of consent, that they have the right to withdraw their consent at any time;

(j) their right to lodge a complaint with the ICO;

(k) whether the provision of personal data is part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the data; and

(l) the existence of any automated decision-making, which produces legal effects concerning the data subject or similarly affects the data subject, including profiling, and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

8.3 If we receive personal data about a data subject from other sources, we shall provide the data subject with the information in paragraph 8.2 above, together with details of the categories of personal data concerned and the source of the personal data (and, if applicable, whether it came from a public source), as soon as possible thereafter.

9 Consent

9.1 Sometimes UCFS will need consent to use a data subject's personal data, for example, where we are sending them certain types of marketing emails, or disclosing sensitive (special category) personal data to a third party.

9.2 Where processing by UCFS is based on consent, we must be able to demonstrate that the data subject has consented to processing of his or her personal data, and that the consent wording and mechanisms used for obtaining and recording consents are compliant with the Data Protection Laws.

9.3 Whenever we request consent for processing, we will:

(a) present the request for consent in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language;

(b) not use 'opt out' boxes or pre-ticked opt-in boxes;

(c) not make services conditional on consent to the processing of personal data that is not necessary for the performance of that contract (for example, marketing);

(d) keep records of consent obtained so we can provide evidence if required;

(e) enable data subjects to withdraw their consent at any time. Data Users should consult with the Data Protection Officer if they receive a notification that a data subject wishes to withdraw his or her consent.

9.4 The data subject shall have the right to withdraw his or her consent at any time. Data Users should consult with the Data Protection Officer if they receive a notification that a data subject wishes to withdraw his or her consent.

9.5 When assessing whether consent is freely given by the data subject, utmost account shall be taken of whether, amongst other things, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

9.6 The processing of children's personal data may require additional parental consent. Data Users should consult the Data Protection Officer in relation to any processing of children's personal data to ensure that relevant compliance steps are addressed.

10 Accurate Data

10.1 We shall ensure that personal data we hold is accurate and kept up to date. We shall check the accuracy of any personal data at the point of collection and at regular intervals afterwards. We shall take all reasonable steps to destroy or amend inaccurate or out-of-date data.

11 Minimal Processing, Data Retention and Security Measures

11.1 UCFS will not collect excess personal data or retain data for longer than we need it. This means:

(a) UCFS will only collect personal data to the extent that it is required for the specific purpose notified to the data subject;

(b) UCFS will not keep personal data longer than is necessary for the purpose for which it was collected (except as required by law);

(c) UCFS will take all reasonable steps to destroy, or erase from our systems, all data which is no longer required, in line with the relevant Record Retention policy.

11.2 We shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, in an effective manner and integrate the necessary safeguards into the processing in order to meet the requirements of the Data Protection Laws and protect the rights of data subjects.

11.3 We shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which is necessary for each specific purpose of the processing is processed. That obligation applies to the amount of personal data collected, the extent of its processing, the period of its storage and its accessibility. In particular, such measures shall ensure that by default personal data is not made accessible without the data subject's intervention to an indefinite number of natural persons.

12 Processing in line with Data Subject's Rights

12.1 We shall process all personal data in line with data subjects' rights, in particular their right to:

(a) be informed of how we process their personal data;

(b) request access to any personal data which we hold about them;

(c) ask to have inaccurate or incomplete personal data amended;

(d) have personal data erased from our systems (where such erasure is not prohibited by law);

(e) not to be subject to automated decisions (i.e. decisions made solely on a computer without human intervention) which that produce legal effects or similarly significantly affect them, unless they have consented or another exception applies;

(f) a right to restrict, 'block' or suppress our use of their personal data and to prevent processing that is likely to cause damage or distress to themselves or anyone else;

(g) receive personal data held about them in a commonly used, machine-readable format, and have the personal data transmitted directly from one data controller to another where it is technically feasible;

(h) object to us profiling them or sending targeted marketing to them; and

(i) where processing of personal data is based on consent (e.g. use of information for direct marketing purposes), a right to withdraw their consent at any time;

13 Data Security

13.1 UCFS will ensure that appropriate measures are taken to keep personal data secure. Data subjects may apply to the courts for compensation if they have suffered damage from such a loss and UCFS may incur large fines if UCFS is in breach of the Data Protection Laws. You can also be criminally liable personally if you steal or recklessly misuse personal data.

13.2 The Data Protection Laws require UCFS to put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction.

13.3 UCFS will maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

(a) **Confidentiality** means that only people who are authorised to use the personal data can access it.

(b) **Integrity** means that personal data should be accurate and suitable for the purpose for which it is processed.

(c) **Availability** means that authorised users should be able to access the personal data if they need it for authorised purposes. Personal data should therefore be stored on the central computer system instead of individual desktops or devices.

13.4 Security procedures include:

(a) **Entry controls.** Any unfamiliar person seen in entry-controlled areas should be reported.

(b) **Encryption.** Any device that holds personal data, including mobile devices and removable media, should be encrypted.

(c) **Secure lockable desks and cupboards.** Desks and cupboards should be kept locked if they hold confidential information of any kind (personal data is always considered confidential).

(d) **Methods of disposal.** Paper documents should be shredded. Digital storage devices should be physically destroyed or wiped when they are no longer required.

(e) **Equipment.** Data Users must ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.

13.5 Generally, to keep personal data secure you must not disclose personal data - in writing or verbally - to anyone not authorised to receive it, whether internal or external, and whether within or outside the workplace.

13.6 In addition to this policy, Data Users must comply with our "Information Security Program and Privacy Policy", which sets out further information about how UCFS keeps all data (including personal data) secure.

14 Data Processors

14.1 We shall only use data processors who provide sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of the Data Protection Laws and ensure the protection of the rights of the data subject.

14.2 Our contracts with data processors shall set out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller.

14.3 Our contracts with data processors shall stipulate that the processor:

(a) processes the personal data only on our documented instructions;

(b) ensures that persons authorised to process the personal data are subject to appropriate confidentiality obligations;

(c) takes all measures required to ensure the security of the personal data;

(d) shall not engage another processor without our prior written consent, and where another processor is engaged, it must be subject to obligations equal to obligations imposed on the original data processor, and the original data processor must remain fully liable to us for performance of its data protection obligations;

(e) assists us by using appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of our obligation to respond to requests for exercising the data subject's rights;

(f) assists us to comply with our obligations under the Data Protection Laws;

(g) shall, at our discretion, delete or return personal data at the end of the service provision (unless required by law to store the personal data);

(h) makes available to us all information necessary to demonstrate its compliance with its data protection obligations in its contract with us; and

(i) shall keep a written record (which may be in electronic form) of all processing activities, which it shall make available to a supervisory authority on request, containing the following information:

(i) the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer;

(ii) the categories of processing carried out;

(iii) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, if applicable, the documentation of appropriate safeguards; and

(iv) where possible, a general description of the technical and organisational security measures which are in place to protect personal data.

15 Transferring Personal Data to a Country Outside the EEA

15.1 We may transfer any personal data we hold to a country outside the European Economic Area (**EEA**), provided that one of the following conditions applies:

(a) the country to which the personal data are transferred ensures an adequate level of protection for the data subjects' rights and freedoms;

(b) the data subject has given his/her consent;

(c) the transfer is necessary for one of the reasons set out in the Data Protection Laws, including the performance of a contract between us and the data subject, or to protect the vital interests of the data subject;

(d) the transfer is legally required on important public interest grounds or for the establishment, exercise or defence of legal claims; or

(e) the transfer is authorised by the relevant data protection authority where we have adduced adequate safeguards with respect to the protection of the data subjects' privacy, their fundamental rights and freedoms, and the exercise of their rights.

15.2 Subject to the requirements in paragraph 15.1 above, personal data we hold may also be processed by employees operating outside the EEA who work for us or for one of our suppliers. Such employees may be engaged in, among other things, the fulfilment of contracts with the data subject, the processing of payment details and the provision of support services.

15.3 We currently transfer employee personal data to our Group Companies as is required for the proper administration of our relationships with our customers and for regulatory purposes as required, and for the adequate management of personnel records by human resources at group level.

Our Group Companies consist of other members of the United Consumer Financial Services Company group of companies, including the United Consumer Financial Services Company, UCFS International holding Company, and The Scott Fetzer Company. The Group Companies are based in the USA and we have entered into the EU style model clauses with each Group Company to ensure that adequate safeguards are in place to protect all personal data shared.

16 Disclosure and Sharing of Personal Data

16.1 We may from time to time share personal data with:

(a) any member of our Group, which means our subsidiaries, our parent company, United Consumer Financial Services Company, and its subsidiaries, as defined in section 1159 of the UK Companies Act 2006;

(b) the Financial Conduct Authority, Prudential Regulatory Authority, and any other relevant regulatory authority;

(c) the Information Commissioner's Office (or any other relevant data protection regulatory authority);

(d) external providers, such as pension, insurance and employee benefits providers;

(e) in the event that UCFS, its business, or substantially all of its assets are acquired by a third party (in which case personal data may form part of the transferred assets); or

(f) in order to comply with legal obligations, or in order to enforce or apply a contract with an individual or other agreement; or to protect our rights, property, or safety of our employees, customers or others. This includes exchanging information with other companies and organisations for the purposes of fraud protection and credit risk reduction.

16.2 We may share personal data with data processors in accordance with the terms of this policy.

16.3 The Data Protection Officer should be notified in advance in case a data sharing agreement needs to be entered into with the third party in order to help ensure that the sharing is compliant with Data Protection Laws.

17 Dealing with Subject Access Requests

17.1 Data subjects may make a formal request for personal data we hold about them. This must be made in writing. Employees who receive a written request should forward it to the Data Protection Officer immediately.

17.2 When receiving telephone enquiries, we shall only disclose personal data we hold on our systems if we verify the caller's identity to make sure that p is only given to a person who is entitled to it. If we are not sure about the caller’s identity and where their identity cannot be checked and we shall suggest that the caller put their request in writing.

17.3 Data Users shall refer a request to the Data Protection Officer for assistance in difficult situations. Data Users should not be bullied into disclosing personal data.

17.4 Where the request for personal data is made in electronic form, we shall provide the information in electronic form where possible, unless otherwise requested by the data subject.

17.5 We shall deal with requests for information without undue delay. Within one month of a request for information, we shall either:

(a) provide the information to the data subject;

(b) if the complexity or number of requests requires, extend the response period by up to a further two months and inform the data subject of such extension; or,

(c) not action the information request, and inform the data subject of the reason for not taking action and of the possibility for lodging a complaint or seeking a judicial remedy.

17.6 If requests for information are manifestly unfounded or excessive (particularly if they are repetitive), we may charge a reasonable fee to carry out the request or refuse to action the request. Employees who suspect they have received such requests should refer them to the Data Protection Officer. Otherwise, initial requests shall be dealt with free of charge, and we may charge a reasonable fee for further requests.

18 Changes to this Policy

18.1 We reserve the right to change this policy at any time. Where appropriate, we shall notify Data Users of this policy of those changes by e-mail.