

## **Wheal Martyn Trust**

### **Data Protection Policy**

#### **Background**

This document is an internal-facing data protection policy setting out the principles and legal conditions that we must satisfy when obtaining, handling, processing, transporting or storing personal data in the course of our operations and activities, including customer, client, supplier and employee data.

#### **Key contacts**

Data Privacy Manager – Office Manager

### **1. Interpretation**

#### **1.1 Definitions:**

**Automated Decision-Making (ADM):** when a decision is made which is based solely on Automated Processing (including profiling) which produces legal effects or significantly affects an individual. The GDPR prohibits Automated Decision-Making (unless certain conditions are met) but not Automated Processing.

**Automated Processing:** any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of Automated Processing.

**Company:** Wheal Martyn Trust, a private limited company by guarantee, registered in England and Wales, registered office Lidn Park, Quarry Crescent, Penningillam Ind Estate, Launceston, Cornwall, PL15 7PF, registered company number 01160460, registered charity number 1001838. References to the Company shall include its subsidiaries.

**Company Personnel:** all employees, workers, contractors, agency workers, consultants, directors, members and others.

**Consent:** agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signifies agreement to the Processing of Personal Data relating to them.

**Data Controller:** the person or organisation that determines when, why and how to process Personal Data. It is responsible for establishing practices and policies in line with the GDPR. We are the Data Controller of all Personal Data relating to our Company Personnel and Personal Data used in for our own purposes.

**Data Privacy Impact Assessment (DPIA):** tools and assessments used to identify and reduce risks of a data processing activity. DPIA can be carried out as part of Privacy by Design and should be conducted for all major system or operational change programs involving the Processing of Personal Data.

**Data Privacy Manager (DPM):** the person required to be appointed in specific circumstances under the GDPR. Where a mandatory DPM has not been appointed, this term means a data protection

manager or other voluntary appointment of a DPM or refers to the Company data privacy team with responsibility for data protection compliance.

**Data Subject:** a living, identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.

**EEA:** the 28 countries in the EU, and Iceland, Liechtenstein and Norway.

**Explicit Consent:** consent which requires a very clear and specific statement (that is, not just action).

**General Data Protection Regulation (GDPR):** the General Data Protection Regulation ((EU) 2016/679). Personal Data is subject to the legal safeguards specified in the GDPR.

**Personal Data:** any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal Data includes Sensitive Personal Data and Pseudonymised Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

**Personal Data Breach:** any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach.

**Privacy by Design:** implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the GDPR.

**Privacy Guidelines:** the Company privacy/GDPR related guidelines provided to assist in interpreting and implementing this Data Protection Policy and Related Policies set out in the schedules.

**Privacy Policies (also referred to as Fair Processing Notices) or Privacy Notices:** separate notices setting out information that may be provided to Data Subjects when the Company collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, employee privacy notices or the website privacy policy) or they may be stand-alone, one time privacy statements covering Processing related to a specific purpose.

**Processing or Process:** any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.

**Pseudonymisation or Pseudonymised:** replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.

**Related Policies:** the Company's policies, operating procedures or processes related to this Data Protection Policy and designed to protect Personal Data annexed below.

**Sensitive Personal Data:** information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and Personal Data relating to criminal offences and convictions.

## **2. Introduction**

This Data Protection Policy sets out how the Company ("we", "our", "us", "the Company") handle the Personal Data of our suppliers, employees, workers and other third parties.

This Data Protection Policy applies to all Personal Data we Process regardless of the media on which that data is stored or whether it relates to past or present employees, workers, customers, clients or supplier contacts, shareholders, website users or any other Data Subject.

This Data Protection Policy applies to all Company Personnel ("you", "your"). You must read, understand and comply with this Data Protection Policy when Processing Personal Data on our behalf and attend training on its requirements. This Data Protection Policy sets out what we expect from you in order for the Company to comply with applicable law. Your compliance with this Data Protection Policy is mandatory. You must also comply with all such Related Policies and Privacy Guidelines. Any breach of this Data Protection Policy may result in disciplinary action of Company Personnel.

This Data Protection Policy (together with Related Policies and Privacy Guidelines) is an internal document and cannot be shared with third parties or regulators without prior authorisation from the DPM.

## **3. Scope**

We recognise that the correct and lawful treatment of Personal Data will maintain confidence in the organisation and will provide for successful operations. Protecting the confidentiality and integrity of Personal Data is a critical responsibility that we take seriously at all times. The Company is exposed to potential fines of up to EUR20 million (approximately £18 million) or 4% of total worldwide annual income, whichever is higher and depending on the breach, for failure to comply with the provisions of the GDPR.

All departments, are responsible for ensuring all Company Personnel comply with this Data Protection Policy and need to implement appropriate practices, processes, controls and training to ensure such compliance.

The DPM is responsible for overseeing this Data Protection Policy and, as applicable, developing Related Policies and Privacy Guidelines.

Please contact the DPM with any questions about the operation of this Data Protection Policy or the GDPR or if you have any concerns that this Data Protection Policy is not being or has not been followed. In particular, you must always contact the DPM in the following circumstances:

- (a) if you are unsure of the lawful basis which you are relying on to process Personal Data (including the legitimate interests used by the Company) (see section 5.1 below);
- (b) if you need to rely on Consent and/or need to capture Explicit Consent (see section 5.2 below);
- (c) if you are unsure about the retention period for the Personal Data being Processed (see section 9 below);
- (d) if you are unsure about what security or other measures you need to implement to protect Personal Data (see section 10.1 below);
- (e) if there has been a Personal Data Breach (section 10.2 below);

- (f) if you are unsure on what basis to transfer Personal Data outside the EEA (see section 11 below);
- (g) if you need any assistance dealing with any rights invoked by a Data Subject (see section 12);
- (h) whenever you are engaging in a significant new, or change in, Processing activity or plan to use Personal Data for purposes others than what it was collected for;
- (i) if you plan to undertake any activities involving Automated Processing including profiling or Automated Decision-Making (see section 13.5 below);
- (j) if you need help complying with applicable law when carrying out direct marketing activities (see section 13.6 below); or
- (k) if you need help with any contracts or other areas in relation to sharing Personal Data with third parties (including our vendors) (see section 13.7 below).

#### **4. Personal data protection principles**

We adhere to the principles relating to Processing of Personal Data set out in the GDPR which require Personal Data to be:

- (a) Processed lawfully, fairly and in a transparent manner (Lawfulness, Fairness and Transparency).
- (b) Collected only for specified, explicit and legitimate purposes (Purpose Limitation).
- (c) Adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (Data Minimisation).
- (d) Accurate and where necessary kept up to date (Accuracy).
- (e) Not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed (Storage Limitation).
- (f) Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage (Security, Integrity and Confidentiality).
- (g) Not transferred to another country without appropriate safeguards being in place (Transfer Limitation).
- (h) Made available to Data Subjects and Data Subjects allowed to exercise certain rights in relation to their Personal Data (Data Subject's Rights and Requests).

We are responsible for and must be able to demonstrate compliance with the data protection principles listed above (Accountability).

#### **5. Lawfulness, fairness, transparency**

##### **5.1 Lawfulness and fairness**

Personal data must be Processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

You may only collect, Process and share Personal Data fairly and lawfully and for specified purposes. The GDPR restricts our actions regarding Personal Data to specified lawful purposes. These

restrictions are not intended to prevent Processing, but ensure that we Process Personal Data fairly and without adversely affecting the Data Subject.

The GDPR allows Processing for specific purposes, some of which are set out below:

- (a) the Data Subject has given his or her Consent;
- (b) the Processing is necessary for the performance of a contract with the Data Subject;
- (c) to meet our legal compliance obligations.;
- (d) to protect the Data Subject's vital interests;
- (e) to pursue our legitimate interests for purposes where they are not overridden because the Processing prejudices the interests or fundamental rights and freedoms of Data Subjects. The purposes for which we process Personal Data for legitimate interests need to be set out in applicable Privacy Notices or Fair Processing Notices.

You must identify and document the legal ground being relied on for each Processing activity.

## **5.2 Consent**

A Data Controller must only process Personal Data on the basis of one or more of the lawful bases set out in the GDPR, which include Consent.

A Data Subject consents to Processing of their Personal Data if they indicate agreement clearly either by a statement or positive action to the Processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If Consent is given in a document which deals with other matters, then the Consent must be kept separate from those other matters.

Data Subjects must be easily able to withdraw Consent to Processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if you intend to Process Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first consented.

Unless we can rely on another legal basis of Processing, Explicit Consent is usually required for Processing Sensitive Personal Data, for Automated Decision-Making and for cross border data transfers. Usually we will be relying on another legal basis (and not require Explicit Consent) to Process most types of Sensitive Data. Where Explicit Consent is required, you must issue a Fair Processing Notice to the Data Subject to capture Explicit Consent.

You will need to evidence Consent captured and keep records of all Consents so that the Company can demonstrate compliance with Consent requirements.

## **5.3 Transparency (notifying data subjects)**

The GDPR requires Data Controllers to provide detailed, specific information to Data Subjects depending on whether the information was collected directly from Data Subjects or from elsewhere. Such information must be provided through appropriate Privacy Notices or Fair Processing Notices which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a Data Subject can easily understand them.

Whenever we collect Personal Data directly from Data Subjects, including for human resources or employment purposes, we must provide the Data Subject with all the information required by the

GDPR including the identity of the Data Controller and DPM, how and why we will use, Process, disclose, protect and retain that Personal Data through a Fair Processing Notice which must be presented when the Data Subject first provides the Personal Data.

When Personal Data is collected indirectly (for example, from a third party or publically available source), you must provide the Data Subject with all the information required by the GDPR as soon as possible after collecting/receiving the data. You must also check that the Personal Data was collected by the third party in accordance with the GDPR and on a basis which contemplates our proposed Processing of that Personal Data.

## **6. Purpose limitation**

Personal Data must be collected only for specified, explicit and legitimate purposes. It must not be further Processed in any manner incompatible with those purposes.

You cannot use Personal Data for new, different or incompatible purposes from that disclosed when it was first obtained unless you have informed the Data Subject of the new purposes and they have Consented where necessary.

## **7. Data minimisation**

Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed.

You may only Process Personal Data when performing your job duties requires it. You cannot Process Personal Data for any reason unrelated to your job duties.

You may only collect Personal Data that you require for your job duties: do not collect excessive data. Ensure any Personal Data collected is adequate and relevant for the intended purposes.

You must ensure that when Personal Data is no longer needed for specified purposes, it is deleted or anonymised in accordance with the Company's data retention guidelines.

## **8. Accuracy**

Personal Data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.

You will ensure that the Personal Data we use and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it. You must check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. You must take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data.

## **9. Storage limitation**

Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed.

You must not keep Personal Data in a form which permits the identification of the Data Subject for longer than needed for the legitimate purpose or purposes for which we originally collected it including for the purpose of satisfying any legal, accounting or reporting requirements.

The Company will maintain retention policies and procedures to ensure Personal Data is deleted after a reasonable time for the purposes for which it was being held, unless a law requires such data to be kept for a minimum time.

You will take all reasonable steps to destroy or erase from our systems all Personal Data that we no longer require in accordance with all the Company's applicable records retention schedules and policies. This includes requiring third parties to delete such data where applicable.

You will ensure Data Subjects are informed of the period for which data is stored and how that period is determined in any applicable Privacy Policy.

## **10. Security integrity and confidentiality**

### **10.1 Protecting Personal Data**

Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful Processing, and against accidental loss, destruction or damage.

We will develop, implement and maintain safeguards appropriate to our size, scope and the nature of our activities, our available resources, the amount of Personal Data that we own or maintain on behalf of others and identified risks (including use of encryption and Pseudonymisation where applicable). We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our Processing of Personal Data. You are responsible for protecting the Personal Data we hold. You must implement reasonable and appropriate security measures against unlawful or unauthorised Processing of Personal Data and against the accidental loss of, or damage to, Personal Data. You must exercise particular care in protecting Sensitive Personal Data from loss and unauthorised access, use or disclosure.

You must follow all procedures and technologies we put in place to maintain the security of all Personal Data from the point of collection to the point of destruction. You may only transfer Personal Data to third-party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

You must maintain data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows:

- (a) Confidentiality means that only people who have a need to know and are authorised to use the Personal Data can access it.
- (b) Integrity means that Personal Data is accurate and suitable for the purpose for which it is processed.
- (c) Availability means that authorised users are able to access the Personal Data when they need it for authorised purposes.

You must comply with and not attempt to circumvent the administrative, physical and technical safeguards we implement and maintain in accordance with the GDPR and relevant standards to protect Personal Data.

### **10.2 Reporting a Personal Data Breach**

The GDPR requires Data Controllers to notify any Personal Data Breach to the applicable regulator and, in certain instances, the Data Subject.

We have put in place procedures to deal with any suspected Personal Data Breach and will notify Data Subjects or any applicable regulator where we are legally required to do so.

If you know or suspect that a Personal Data Breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the DPM. You should preserve all evidence relating to the potential Personal Data Breach.

## **11. Transfer limitation**

The GDPR restricts data transfers to countries outside the EEA in order to ensure that the level of data protection afforded to individuals by the GDPR is not undermined. You transfer Personal Data originating in one country across borders when you transmit, send, view or access that data in or to a different country.

You may only transfer Personal Data outside the EEA if one of the following conditions applies:

- (a) the European Commission has issued a decision confirming that the country to which we transfer the Personal Data ensures an adequate level of protection for the Data Subjects' rights and freedoms;
- (b) appropriate safeguards are in place such as binding corporate rules (BCR), standard contractual clauses approved by the European Commission, an approved code of conduct or a certification mechanism, a copy of which can be obtained from the DPM;
- (c) the Data Subject has provided Explicit Consent to the proposed transfer after being informed of any potential risks; or
- (d) the transfer is necessary for one of the other reasons set out in the GDPR including the performance of a contract between us and the Data Subject, reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the Data Subject where the Data Subject is physically or legally incapable of giving Consent and, in some limited cases, for our legitimate interest.

## **12. Data Subject's rights and requests**

Data Subjects have rights when it comes to how we handle their Personal Data. These include rights to:

- (a) withdraw Consent to Processing at any time;
- (b) receive certain information about the Data Controller's Processing activities;
- (c) request access to their Personal Data that we hold;
- (d) prevent our use of their Personal Data for direct marketing purposes;
- (e) ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or Processed or to rectify inaccurate data or to complete incomplete data;
- (f) restrict Processing in specific circumstances;
- (g) challenge Processing which has been justified on the basis of our legitimate interests or in the public interest;
- (h) request a copy of an agreement under which Personal Data is transferred outside of the EEA;
- (i) object to decisions based solely on Automated Processing, including profiling (ADM);



- (j) prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else;
- (k) be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;
- (l) make a complaint to the supervisory authority; and
- (m) in limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine readable format.

You must verify the identity of an individual requesting data under any of the rights listed above (do not allow third parties to persuade you into disclosing Personal Data without proper authorisation).

You must immediately forward any Data Subject request you receive to the DPM and comply with the Company's Data Subject response process.

### **13. Accountability**

- 13.1 The Data Controller must implement appropriate technical and organisational measures in an effective manner, to ensure compliance with data protection principles. The Data Controller is responsible for, and must be able to demonstrate, compliance with the data protection principles.

The Company must have adequate resources and controls in place to ensure and to document GDPR compliance including:

- (a) appointing a suitably qualified data protection officer (where necessary) and an executive accountable for data privacy;
- (b) implementing Privacy by Design when Processing Personal Data and completing DPIAs where Processing presents a high risk to rights and freedoms of Data Subjects;
- (c) integrating data protection into internal documents including this Data Protection Policy, Related Policies, Privacy Guidelines and Privacy Policy;
- (d) regularly training Company Personnel on the GDPR, this Data Protection Policy, Related Policies and Privacy Guidelines and data protection matters including, for example, Data Subject's rights, Consent, legal basis, DPIA and Personal Data Breaches. The Company must maintain a record of training attendance by Company Personnel; and
- (e) regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

### **13.2 Record keeping**

The GDPR requires us to keep full and accurate records of all our data Processing activities.

You must keep and maintain accurate corporate records reflecting our Processing including records of Data Subjects' Consents and procedures for obtaining Consents.

These records should include, at a minimum, the name and contact details of the Data Controller and the DPM, clear descriptions of the Personal Data types, Data Subject types, Processing activities, Processing purposes, third-party recipients of the Personal Data, Personal Data storage locations,

Personal Data transfers, the Personal Data's retention period and a description of the security measures in place.

### **13.3 Training and audit**

We are required to ensure all Company Personnel have undergone adequate training to enable them to comply with data privacy laws. We must also regularly test our systems and processes to assess compliance.

You must undergo all mandatory data privacy related training and ensure your team undergo similar mandatory training.

You must regularly review all the systems and processes under your control to ensure they comply with this Data Protection Policy and check that adequate governance controls and resources are in place to ensure proper use and protection of Personal Data.

### **13.4 Privacy By Design and Data Protection Impact Assessment (DPIA)**

We are required to implement Privacy by Design measures when Processing Personal Data by implementing appropriate technical and organisational measures (like Pseudonymisation) in an effective manner, to ensure compliance with data privacy principles.

You must assess what Privacy by Design measures can be implemented on all programs/systems/processes that Process Personal Data by taking into account the following:

- (a) the state of the art;
- (b) the cost of implementation;
- (c) the nature, scope, context and purposes of Processing; and
- (d) the risks of varying likelihood and severity for rights and freedoms of Data Subjects posed by the Processing.

Data controllers must also conduct DPIAs in respect to high risk Processing.

You should conduct a DPIA (and discuss your findings with the DPM) when implementing major system or business change programs involving the Processing of Personal Data including:

- (e) use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);
- (f) Automated Processing including profiling and ADM;
- (g) large scale Processing of Sensitive Data; and
- (h) large scale, systematic monitoring of a publicly accessible area.

A DPIA must include:

- (i) a description of the Processing, its purposes and the Data Controller's legitimate interests if appropriate;
- (j) an assessment of the necessity and proportionality of the Processing in relation to its purpose;
- (k) an assessment of the risk to individuals; and

- (l) the risk mitigation measures in place and demonstration of compliance.

### **13.5 Automated Processing (including profiling) and Automated Decision-Making**

Generally, ADM is prohibited when a decision has a legal or similar significant effect on an individual unless:

- (a) a Data Subject has Explicitly Consented;
- (b) the Processing is authorised by law; or
- (c) the Processing is necessary for the performance of or entering into a contract.

If certain types of Sensitive Data are being processed, then grounds (b) or (c) will not be allowed but such Sensitive Data can be Processed where it is necessary (unless less intrusive means can be used) for substantial public interest like fraud prevention.

If a decision is to be based solely on Automated Processing (including profiling), then Data Subjects must be informed when you first communicate with them of their right to object. This right must be explicitly brought to their attention and presented clearly and separately from other information. Further, suitable measures must be put in place to safeguard the Data Subject's rights and freedoms and legitimate interests.

We must also inform the Data Subject of the logic involved in the decision making or profiling, the significance and envisaged consequences and give the Data Subject the right to request human intervention, express their point of view or challenge the decision.

A DPIA must be carried out before any Automated Processing (including profiling) or ADM activities are undertaken.

### **13.6 Direct marketing**

We are subject to certain rules and privacy laws when marketing to our customers.

For example, a Data Subject's prior consent is required for electronic direct marketing (for example, by email, text or automated calls). The limited exception for existing supporters known as "soft opt in" allows organisations to send marketing texts or emails if they have obtained contact details in the course of a sale to that person or when obtaining a donation or similar commitment, they are marketing similar products, services or campaigns, and they gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent message.

The right to object to direct marketing must be explicitly offered to the Data Subject in an intelligible manner so that it is clearly distinguishable from other information.

A Data Subject's objection to direct marketing must be promptly honoured. If an individual opts out at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

### **13.7 Sharing Personal Data**

Generally we are not allowed to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place.

You may only share the Personal Data we hold with another employee, agent or representative of our group (which includes our subsidiaries and our ultimate holding company along with its subsidiaries) if the recipient has a job-related need to know the information and the transfer complies with any applicable cross-border transfer restrictions.

You may only share the Personal Data we hold with third parties, such as our service providers if:

- (a) they have a need to know the information for the purposes of providing the contracted services;
- (b) sharing the Personal Data complies with the Privacy Notice provided to the Data Subject and, if required, the Data Subject's Consent has been obtained;
- (c) the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;
- (d) the transfer complies with any applicable cross border transfer restrictions; and
- (e) a fully executed written contract that contains GDPR approved third party clauses has been obtained.

#### **14. Changes to this Data Protection Policy**

We reserve the right to change this Data Protection Policy at any time without notice to you so please check back regularly to obtain the latest copy of this Data Protection Policy. We last revised this Data Protection Policy on [DATE].

This Data Protection Policy does not override any applicable national data privacy laws and regulations in countries where the Company operates.

## **Privacy Guidelines - data protection dos and don'ts**

### **Privacy and data protection**

- Before using any individual's personal information, such as name, address or telephone number, ensure that it is lawful to do so, for example, by obtaining the individual's consent.
- Only use personal information in a way that falls within an individual's reasonable expectations.
- Before transferring personal information outside the Company, or within the Company but outside the EEA, ensure that it is lawful to do so, for example, by obtaining the individual's consent.
- Do not send emails or SMS for marketing purposes without obtaining authorisation from the DPM first.

### **IT and data security**

- Always keep your password and user name secure and do not share them.
- Always lock your PC while it is unattended.
- Do not open email attachments from an unknown source.
- Do not download programs or games, or run any sent by email.
- Do not download Company data onto any laptop unless authorized by your manager.
- Ensure that any personal information held on a laptop is encrypted.
- When taking a laptop with you to another country for work, ensure that it only contains the customer information you need.
- If your laptop is lost or stolen, contact your manager immediately.
- Any device that is left unattended must be locked or logged out to prevent unauthorised access.
- Leave nothing on display that may contain access information, such as login names or passwords.
- Ensure that portable devices in their custody are not exposed to opportunistic theft.
- Documents that contain personal information should not be left on desks unattended and should be removed from view when unsupervised.
- Documents should be collected from printers as soon as they are produced and not left where they can be read by passers-by.
- At the end of each day, all documents that contain any personal information (information about living, identifiable individuals) will be:
  - Cleared from every desk
  - Cleared from trays or other 'inboxes' (or the trays themselves moved to a secure locations)
  - Cleared from printers, photocopiers or fax machines
  - Stored in a locked cupboard, cabinet, set of draws or safe overnight.
- The IT department will deploy up-to-date anti-virus software to all users. Users must therefore ensure any portable IT device is connected to the network a minimum of three times every week to enable the anti-virus software to be updated. Users can log in remotely to the network and systems.
- Users are responsible for protecting Company personal information and IT devices against physical security threats.

- At home: this means located out of sight of the casual visitor, family members or others who share your accommodation. Ideally any home office area should be separate from the rest of the house.
- In transit: this means not being left unattended for any period of time, including when visiting the toilet, buying refreshments, or otherwise being away from the information or device. If it is unavoidable that information is left unattended ensure it is locked away and out of sight e.g. in the boot of the car.

### **Privacy and data protection: when inputting personal information into the Company's CRM database**

- These guidelines are in addition to the Company's rules on privacy and data protection and any rules or guidelines specific to your office.
- Please do not enter negative comments on any individual, including customers, employees or suppliers, onto the CRM database. If there is an issue which other people need to be aware of, for example, you were not satisfied with the performance of a supplier, state "Contact [YOUR NAME] before contacting this person".
- Keep any business card given by a contact whose information you propose inputting into the CRM database.
- If a person indicates that they do not want to receive marketing communications, check the relevant on the CRM database to indicate they have opted out or withdrawn consent. Marketing communications include newsletters and other updates or publications, and invitations to events. You should also check this box if a person does not wish to receive a specific type of marketing communication, for example, invitations to events. In any of these cases, ensure that the person's wishes are respected by notifying all internal contacts who need to know.
- Before entering sensitive personal information about an individual on the CRM database, ensure that it is lawful to do so, for example, by obtaining the individual's explicit written consent. Sensitive personal information generally includes:
  - racial or ethnic origin;
  - political opinions;
  - religious or philosophical beliefs;
  - trade union membership;
  - physical or mental health;
  - sexual life;
  - criminal offences; and
  - financial information.
- If a person provides information for the personal use of particular individuals within the organization only (for example, a home address or telephone number), or for a specific purpose or duration, you should ensure that these use restrictions are entered on the CRM database.

### **Privacy and data protection: do's and don'ts when using email**

- These guidelines are in addition to the Company's rules on privacy and data protection and any rules or guidelines specific to your office.
- Before sending an email, please think about what you are trying to achieve and decide on the best communication method to use. For example, a telephone call might be more effective.

- Keep your message brief and relevant and do not send unnecessary copies of the message.
- When writing your emails, always assume that they may have to be disclosed to a court or regulator, because in some circumstances that could happen.
- Always write your emails as if they are permanent, because even when they have been deleted they can often still be retrieved and may be disclosable to a court or regulator.
- Your emails, even if marked private or confidential, might also be viewed by network supervisors or management when lawful to do so.
- Uphold the privacy of others by observing the Company's rules and guidelines.
- Avoid asking for sensitive personal information unless necessary for a legal or operational purpose, or passing on sensitive personal information about somebody else. Sensitive personal information includes:
  - racial or ethnic origin;
  - political opinions;
  - religious or philosophical beliefs;
  - trade union membership;
  - physical or mental health;
  - sexual life;
  - criminal offences; and
  - financial information.
- If it is necessary to ask for sensitive personal information for an operational purpose, contact the DPM first.
- Consider sending confidential information by secure email.
- Do not make negative comments about any individual, including supporters, customers, employees or suppliers. If you feel that there is a problem which other people need to be aware of, then sending an email is not the appropriate way of doing this. Speak to your manager first about the next steps.
- Do not send any email which might be construed as offensive or discriminatory and do not download obscene material.
- Please tidy your inbox, outbox and folders regularly. Do not store messages or attachments longer than necessary.

## **Privacy Guidelines - sharing personal information**

Personal information must only be shared by following an agreed procedure as below:

- Users are to contact the appropriate manager for advice before releasing any personal information if they are unclear about the procedures or protocols to follow.
- Users should be aware of their responsibilities when sharing personal information and they should be able to:-
  - Justify the sharing
  - Maintain security to the level expected by the classification of the personal information, whether the sharing is in person, made verbally, by SFTP (Secure File Transfer Protocol) by email, fax, or post

### Sharing requirements:

The User must, before sharing or sending the personal information, be satisfied:-

- Of the identity of the recipient; this includes internal colleagues, external third parties and individuals
- Of the contact details of the recipient – e.g. email address; fax number; phone number, SFTP site address.
- Of the recipient's need to know and/or their entitlement to the personal information – seeking written proof where necessary
- That they are authorised to share the personal information.

If in doubt, the personal information should not be shared and further details and assurance must be sought. For example:-

- Return the intended recipient's call using a known telephone number.
- Verify the intended recipient's email address by checking against a known source.
- Verify the intended recipient's postal address by checking against a known source (e.g. seeking copies of formal, official headed documentation)
- Verify intended recipients SFTP site address by sending a test file

The personal information to be shared must:-

- Only be that required to fulfil the purpose or purposes behind the proposed sharing
- Only be that defined on any court order or other document compelling disclosure
- Be accurate

### Disclosure of information – email

- Only Company email accounts and not personal email accounts must be used for Company business. If the email recipient is outside the Company email should not contain personal information without the permission of the person the information is about/refers to.



- Care should be taken when addressing all emails to prevent accidental sharing to unintended recipients. Employees should double check each email address before pressing send.
- Distribution lists should not be used to send personal information and should be checked monthly, and updated as soon as the User is informed of a change in distribution and/or email address.
- If sending to multiple external email addresses Bcc them rather than Cc so that recipients are not aware of others information.
- If personal data is emailed to an outside organisation it must be done in a secure manner.

#### Disclosure of information – oral

Users must protect the interests of the individuals subject to the personal information when discussing personal information in conversations, on the telephone or when recording information on voicemail, answering machines, video or audio devices. Users must ensure they are aware of their surroundings when having any private conversation.

#### Disclosure of information – fax

Users must ensure that the recipient of a fax is aware that it is being sent if it contains any personal information. A fax cover sheet must be used stating who the fax is from, contact details and a disclaimer.