Data Protection Policy

Document contents

Purpose

This document is part of the Appointedd ISMS.
The policy provides information about the Data Protection principles and how Appointedd expects personal information to be handled. It outlines the roles and responsibilities of Appointedd Employees in relation to Data Protection. This policy has been developed to manage the way in which Appointedd complies with its Data Protection obligations and provide individuals with assurance that there are effective governance arrangements in place.

This policy is reviewed at least annually and may be reviewed ad hoc as needed, and is approved by the Information Security Management (ISM) Team. This policy has been developed to manage the way in which Appointedd complies within the ISO 27001 standard.

Policy statement

Everyone has rights with regard to how their personal information is handled. During the course of Appointedd business activities we will collect, store and process personal information, and we recognise the need to treat it in an appropriate and lawful manner.

The types of information that we may be required to handle include details such as;

- Name.
- Address.
- Email address.
- Telephone number.
- Company name.
- Website.
- IP Address.

The information, which may be on a computer database or other media, is subject to certain legal safeguards specified in the General Data Protection Regulation (GDPR) and the UK Data Protection Act (DPA). This legislation imposes restrictions on how we may use that information. This policy will apply to all employees of Appointedd when processing personal data for and on behalf of

Appointedd. Any breach of this policy will be taken seriously and may result in disciplinary action.

Definition of data protection terms

1. General Data Protection Regulation (GDPR) 2016, effective from 25th May 2018, is the EU law on data protection and privacy for all individuals with the European Union (EU) and the European Economic Area (EEA). The GDPR aims primarily to give control back to citizens and residents over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU.

2. Data Protection Act 2018 (DPA) is the main UK legislation which makes provision for GDPR into UK law. It also provides derogations for certain processing activities.

3. Data is information which is stored electronically, on a computer, or in certain paper-based filing systems.

4. Anonymised information is information from which no individual can be identified.

5. Data subjects for the purpose of this policy include all living individuals about whom we hold personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal data.

6. Personal data means data relating to a living individual who can be identified from that data and other information in our possession, or is likely to come into our possession. Personal data can be factual (such as a name, address or date of birth) or it can be an opinion (such as a performance appraisal).

7. Data controllers are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They have a responsibility to establish practices and policies in line with the Act. We are the data controller of all personal data used within

the Appointedd.

8. Data users include all employees whose work involves using personal data. Data users have a duty to protect the information they handle by following our data protection and security policies at all times.

9. Data processors include any person who processes personal data on behalf of Appointedd. Employees of data controllers are excluded from this definition but it could include suppliers which handle personal data on our behalf.

10. Processing is any activity that involves the use of the 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 transferring personal data to third parties.

11. Special Category personal data includes information about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic or biometric data, data concerning health or data concerning a person's sex life or sexual orientation.

12. Data sharing relates to the disclosure of data from one or more organisations to a third party organisation(s), or the sharing of data between different parts of an organisation. It can take the form of systematic, routine data sharing where the same data sets are shared between the same organisations for an established purpose; and exceptional, one off decisions to share data for any of a range of purposes.

13. Data sharing agreements/protocols set out a common set of rules to be adopted by the various organisations involved in a data sharing operation.

14. Privacy notice is information provided to data subjects in relation to how their personal information is collected, handled and processed.

15. Data Protection Impact Assessment (DPIA) is a comprehensive process for

determining the privacy, confidentiality and security risks associated with the collection, use and disclosure of personal data.

Data protection principles

Employees of Appointedd that process personal data must comply with the enforceable principles of data protection that are set out under article 5 of the GDPR. These provide that personal data must be:

- Processed lawfully, fairly, and in a transparent manner.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up to date.
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

There are also additional requirements set outside of the main principles, these include:

- Accountability; Appointedd shall be responsible for, and be able to demonstrate compliance with all of the principles listed above.
- International transfers; personal data shall not be processed in a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.
- Individual's Rights; covered within this policy in a section below.

Lawful, fair & transparent data processing

The Regulation is not intended to prevent the processing of personal data, but

seeks to ensure that personal data is processed lawfully, fairly and transparently, without adversely affecting the rights of the data subject.

The data subject/s must be provided with a privacy notice that confirms;

- who the data controller is, in this case Appointedd,
- the purpose for which the data is to be processed, and
- the identities of anyone to whom the data may be disclosed or transferred.

Appointedd's Privacy Notice is available on the corporate website.

The GDPR states that processing of personal data shall be lawful if at least one of the following applies.

- The data subject has given consent to the processing of their personal data for one or more specific purposes;
- The processing is necessary for the performance of a contract to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering into a contract with them;
- The processing is necessary for compliance with a legal obligation to which the data controller is subject;
- The processing is necessary to protect the vital interests of the data subject or of another natural person;
- The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller; or
- The processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Specified, Explicit, and Legitimate Purposes

The Company collects and processes the personal data as per the following

Type of Data	Purpose of Data

Name and contact	To allow Company to communicate and deliver products/services.
Data subject address	To allow Company to communicate and deliver products/services.
Email address	To allow Company to communicate and deliver products/services.
Phone Number	To allow Company to communicate and deliver products/services.
IP Address	Access logs for debugging purposes.
Website	To link to the business website.
Company name	To allow Company to communicate and deliver products/services.

- The Company only collects, processes, and holds this personal data for the specific purposes set out in the table above (or for other purposes expressly permitted by the GDPR).
- Data subjects are kept informed at all times of the purpose or purposes for which the Company uses their personal data.

Adequate, Relevant, and Limited Data Processing

- The Company will only collect and process personal data for and to the extent necessary for the specific purpose or purposes of which data subjects have been informed (or will be informed) as above in the table.

Accuracy of Data

- The Company shall ensure that all personal data collected, processed, and held by it is kept accurate and up-to-date. This includes, but is not limited to, the rectification of personal data at the request of a data subject.

    - Data subjects have the right to require the Company to rectify any of their personal data that is inaccurate or incomplete.
    - The Company shall rectify the personal data in question, and inform the data subject of that rectification, within one month of the data subject informing the Company of the issue. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.
    - In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification that must be made to that personal data.
- The accuracy of personal data shall be checked when it is collected and at regular intervals thereafter. If any personal data is found to be inaccurate or out-of-date, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

Kept Informed

- Where personal data is collected directly from data subjects, those data subjects will be informed of its purpose at the time of collection; and
- Where personal data is obtained from a third party, the relevant data subjects will be informed of its purpose
    - if the personal data is used to communicate with the data subject, when the first communication is made; or
    - if the personal data is to be transferred to another party, before that transfer is made; or
    - as soon as reasonably possible and in any event not more than one month after the personal data is obtained.
- The following information shall be provided:
    - Details of the Company including, but not limited to, the identity of its Data Protection Officer;
    - The purpose(s) for which the personal data is being collected, processed and the legal basis justifying that collection and processing;
    - Where applicable, the legitimate interests upon which the Company is justifying its collection and processing of the personal data;

- Where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed;
- Where the personal data is to be transferred to one or more third parties, details of those parties;
- Where the personal data is to be transferred to a third party that is located outside of the European Economic Area (the "EEA"), details of that transfer, including but not limited to the safeguards in place
- Details of data retention;
- Details of the data subject's rights under the GDPR;
- Details of the data subject's right to withdraw their consent to the Company's processing of their personal data at any time;
- Details of the data subject's right to complain to the Information Commissioner's Office (the "supervisory authority" under the GDPR);
- Where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the personal data and details of any consequences of failing to provide
- Details of any automated decision-making or profiling that will take place using the personal data, including information on how decisions will be made, the significance of those decisions, and any consequences.

Secure Processing

The Company shall ensure that all personal data collected, held, and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction, or damage.

The Company shall ensure that the following measures are taken with respect to the collection, holding, and processing of personal data:

- All employees, agents, contractors, or other parties working on behalf of the Company shall be made fully aware of both their individual responsibilities and the Company's responsibilities under the GDPR and under this Policy, and shall be provided with a copy of this Policy;

- Only employees, agents, sub-contractors, or other parties working on behalf of the Company that need access to, and use of, personal data in order to carry out their assigned duties correctly shall have access to personal data held by the Company;
- All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be appropriately trained to do so;
- All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be appropriately supervised;
- All employees, agents, contractors, or other parties working on behalf of the Company handling personal data shall be required and encouraged to exercise care, caution, and discretion when discussing work-related matters that relate to personal data, whether in the workplace or otherwise;
- Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed;
- All personal data held by the Company shall be reviewed periodically;
- The performance of those employees, agents, contractors, or other parties working on behalf of the Company handling personal data shall be regularly evaluated and reviewed;
- All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be bound to do so in accordance with the principles of the GDPR and this Policy by contract;
- All agents, contractors, or other parties working on behalf of the Company handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of the Company arising out of this Policy and the GDPR; and
- Where any agent, contractor or other party working on behalf of the Company handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless the Company against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.
- No personal data may be shared informally and if an employee, agent, sub-contractor, or other party working on behalf of the Company requires access to any personal data that they do not already have access to, such access should be formally requested from the Data Protection Officer, DataCo International UK Limited.

- No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of the Company or not, without the authorisation of the Data Protection Officer, DataCo International UK Limited.
- Personal data must be handled with care at all times and should not be left unattended or on view to unauthorised employees, agents, sub-contractors, or other parties at any time;
- If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it; and
    - Where personal data held by the Company is used for marketing purposes, it shall be the responsibility of DataCo International UK Limited to ensure that the appropriate consent is obtained and that no data subjects have opted out, whether directly or via third-party services.

The Company shall ensure that the following measures are taken with respect to the storage of personal data:

- All electronic copies of personal data should be stored securely using passwords and data encryption;
- All hard copies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet, or similar;
- All personal data stored electronically should be backed up with backups stored offsite. All backups should be encrypted;
- No personal data should be stored on any mobile device (including, but not limited to, laptops, tablets, and smartphones), whether such device belongs to the Company or otherwise without the formal written approval of the Data Protection Officer, DataCo International UK Limited, and, in the event of such approval, strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary; and
- No personal data should be transferred to any device personally belonging to an employee and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of the Company where the party in question has agreed to comply fully with the

letter and spirit of this Policy and of the GDPR (which may include demonstrating to the Company that all suitable technical and organisational measures have been taken).

Accountability

- The Company's Data Protection Officer is DataCo International UK Limited - privacy@dataguard.co.uk.

- The Data Protection Officer shall be responsible for overseeing the implementation of this Policy and for monitoring compliance with this Policy, the Company's other data protection-related policies, and with the GDPR and other applicable data protection legislation.

- The Company shall keep internal records of all personal data collection, holding, and processing, which shall incorporate the following information:
    - The name and details of the Company, its Data Protection Officer, and any applicable third-party data processors
    - The purposes for which the Company collects, holds, and processes personal data;
    - Details of the categories of personal data collected, held, and processed by the Company, and the categories of data subject to which that personal data relates;
    - Details of any transfers of personal data to non-EEA countries including all mechanisms and security safeguards;
    - Details of how long personal data will be retained by the Company; and
    - Detailed descriptions of all technical and organisational measures taken by the Company to ensure the security of personal data.

International Transfers

- The Company may from time to time transfer ('transfer' includes making available remotely) personal data to countries outside of the EEA.
- The transfer of personal data to a country outside of the EEA shall take place only if one or more of the following applies:

- The transfer is to a country, territory, or one or more specific sectors in that country (or an international organisation), that the European Commission has determined ensures an adequate level of protection for personal data;
- The transfer is to a country (or international organisation) which provides appropriate safeguards in the form of a legally binding agreement between public authorities or bodies; binding corporate rules; standard data protection clauses adopted by the European Commission; compliance with an approved code of conduct approved by the supervisory authority (e.g. the Information Commissioner's Office); certification under an approved certification mechanism (as provided for in the GDPR); contractual clauses agreed and authorised by the competent supervisory authority; or provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority;
- The transfer is made with the informed consent of the relevant data subject(s);
- The transfer is necessary for the performance of a contract between the data subject and the Company (or for pre-contractual steps taken at the request of the data subject);
- The transfer is necessary for important public interest reasons;
- The transfer is necessary for the conduct of legal claims;
- The transfer is necessary to protect the vital interests of the data subject or other individuals where the data subject is physically or legally unable to give their consent; or
- The transfer is made from a register that, under UK or EU law, is intended to provide information to the public and which is open for access by the public in general or otherwise to those who are able to show a legitimate interest in accessing the register.

Individual's Rights

The GDPR provides the following rights for individuals:

- The right to be informed
- The right of access

- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

The legal basis being relied upon to use someone's personal information will affect the rights that the individual has in relation to their information. For example if relying upon the consent of the person to use their personal data, then the right to have their personal information erased is stronger. As such it is important to identify the correct legal basis from the outset.

Data security

Appointedd ensures that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against accidental loss of, or damage to, personal data.

All alleged breaches of the data protection policy must be reported immediately to the Company's Data Protection Officer.

- If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the Data Protection Officer must ensure that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.
- In the event that a personal data breach is likely to result in a high risk to the rights and freedoms of data subjects, the Data Protection Officer must ensure that all affected data subjects are informed of the breach directly and without undue delay.
- Data breach notifications shall include the following information:
    - The categories and approximate number of data subjects concerned;
    - The categories and approximate number of personal data records concerned;

    - The name and contact details of the Company's data protection officer (or another contact point where more information can be obtained);
    - The likely consequences of the breach;
    - Details of the measures taken or proposed to be taken, by the Company to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

The Regulation requires Appointedd 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. Personal data may only be transferred to a third-party data processor if the respective third party agrees to comply with those procedures and policies, or if they put in place adequate security measures themselves.

Maintaining data security means guaranteeing the confidentiality, integrity and availability of the personal data. defined as follows:

- Confidentiality means that only people who are authorised to use the data can access it.
- Integrity means that personal data should be accurate and suitable for the purpose for which it is processed.
- Availability means that authorised users should be able to access the data if they need it for authorised purposes.

Data Retention

- The Company shall not keep personal data for any longer than is necessary in light of the purpose or purposes for which that personal data was originally collected, held, and processed.
- When personal data is no longer required, all reasonable steps will be taken to erase or otherwise dispose of it without delay.
- Full details of the Company's approach to data retention can be found in the data retention policy.