DATA PROTECTION POLICY

CONTENTS

CLAUSE

SCHEDULE

1.0 POLICY STATEMENT

1. Everyone has rights with regard to the way in which their personal data is handled. During the course of our activities we collect, store and process personal data about our customers, suppliers and other third parties, as well as our employees and other workers, and we recognise that the correct and lawful treatment of this data will maintain confidence in our organisation and will assist us to achieve success in our business operations.
2. Employees and other individuals who handle personal data within our organisation are obliged to comply with this policy when processing personal data on our behalf.

2.0 ABOUT THIS POLICY

1. Personal data which is held on a computer or other electronic device, and in some cases in paper files, is subject to certain legal safeguards specified in the Data Protection Act 1998 (the "DPA") and other regulations. As from 25th May 2018 the DPA will be replaced by the EU General Data Protection Regulation ("GDPR"), supplemented by UK legislation currently going through Parliament ("New DPA"). These laws are together referred to in this policy document as the "Data Protection Legislation".
2. The Data Protection Legislation is not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject.
3. This policy sets out the basis on which we process any personal data that we collect from data subjects or other sources outside of our organisation. For the ways in which we process personal data about our own employees and other workers, please see the separate policy "Processing Employee Data".
4. This policy does not form part of any employee's contract of employment and may be amended at any time. Nevertheless, any breach of this policy may result in disciplinary action, as well as possible personal liability.
5. This policy has been approved by the 8build Board. It sets out rules on data protection and the legal conditions that must be satisfied when we collect, handle, process, store and transfer personal data.
6. The Data Controller is responsible for ensuring compliance with the Data Protection Legislation and with this policy. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the Data Controller.

3.0 DEFINITION OF DATA PROTECTION TERMS

1. Data is information which is stored electronically, on a computer or other device, or in certain paper-based filing systems.
2. Data subjects 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 information.
3. Personal data means data relating to a living individual who can be identified, directly or indirectly, from that data (or from that data and other information in our possession), in particular by reference to an identifier such as a name, an identification number, location data or an online identifier. Personal data can be factual (for example, a name, address, email address or date of birth or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person) or it can be an opinion about that person, their actions and behaviour.

4. Data controllers are the people who, or organisations which, determine the purposes and means of processing personal data. They are responsible for establishing practices and policies in line with the Data Protection Legislation. We are the data controller of all personal data used in our business for our own commercial purposes other than (for example) where we process data in the context of providing services to a third party who is the data controller, in which case we will be a data processor.
5. Data users are those of our employees or other workers 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.
6. Data processors include any person or organisation (other than a data user) that processes personal data on our behalf and on our instructions. Data processors will include suppliers that handle personal data on our behalf.
7. Processing is any operation or set of operations performed on personal data or on sets of personal data, whether or not by automated means. It includes the collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction or destruction of the data.
8. Sensitive personal data (referred to under the GDPR as "special categories of personal data") includes information revealing a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, as well as data concerning a person's health or sex life or sexual orientation. Sensitive personal data, as previously defined, can only be processed with the explicit consent of the person concerned. Under the DPA, sensitive personal data also includes information 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. Under the GDPR and the New DPA, similar conditions apply to processing of personal data about criminal convictions and offences or related security measures.
9. Third country means a country outside the European Union (or the EEA).

4.0 DATA PROTECTION PRINCIPLES

1. Data controllers are responsible for ensuring and demonstrating that data processing is performed in accordance with the requirements of the Data Protection Legislation ("Data Protection Principles"). These provide that personal data must be
    a. processed fairly and lawfully and in a transparent manner;
    b. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
    c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
    d. accurate and, where necessary, kept up to date;
    e. kept in a form which permits identification of data subjects for no longer than necessary for the purpose;
    f. 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.
2. In addition, personal data must not be transferred to people or organisations situated in countries without adequate protection for personal data.

3. When processing personal data as the data controller in the course of our business, we will ensure that those requirements are met, and all Data Users must therefore take account of the contents of this policy document.

5.0 FAIR AND LAWFUL PROCESSING

1. For personal data to be processed lawfully, they must be processed on the basis of one of the legal grounds set out in the Data Protection Legislation. These include, among other things, where:
    a. the data subject has given consent to the processing, or
    b. the processing is necessary for the performance of a contract with the data subject, or
    c. the processing is necessary for the compliance with a legal obligation to which the data controller is subject, or
    d. the processing is necessary for the legitimate interests of the data controller or a third party (except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data).
2. When sensitive personal data is being processed (including personal data about criminal convictions etc), additional conditions must be met and appropriate care will be taken.
3. It is important to note that when the data subject's consent is relied on as a lawful basis for processing, it has to be freely given, specific, informed and unambiguous. In addition:
    a. consent requires some form of clear affirmative action;
    b. silence, pre-ticked boxes or inactivity does not constitute consent;
    c. if the data subject's consent is given in a context which also concerns other matters, the request for consent must be presented so it is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language;
    d. consent must be verifiable; and
    e. individuals have a right to withdraw their consent at any time, as easily as they gave it.

6.0 PERSONAL DATA WE MAY COLLECT AND PROCESS

4. In the course of our business, we may collect and process the personal data set out in the Schedule. This may include data we receive directly from a data subject (for example, by completing forms or by corresponding with us by mail, phone, email or otherwise) and data we receive from other sources (including, for example, business partners, sub-contractors in technical, payment and delivery services, credit reference agencies and others).
5. We will only process personal data of the types and for the specific purposes set out in the Schedule or for any other purposes specifically permitted by the Data Protection Legislation. We must also ensure that our processing is based on the lawful basis set out there, and is not retained for longer than the period set out there, and that personal data is not transferred to third parties other than those specified in the Schedule.

7.0 NOTIFYING DATA SUBJECTS

1. If we collect personal data directly from data subjects, we must inform them of:
    a. our identity and contact details;
    b. the purpose or purposes for which we intend to process that personal data, as well as our legal basis for doing so;
    c. where we are processing the personal data on the basis of legitimate interests, what those interests are;
    d. the third parties, or categories of third parties, if any, with which we will share or to which we will disclose that personal data;
    e. If we intend to transfer the personal data to a Third Country, the adequacy (or otherwise) of the data protection laws there, and safeguards to be used to protect the personal data (and how the data subject can access these safeguards).
2. In addition, the following information must also be provided at the time of collection, where this is necessary in order to ensure fair and transparent processing:
    a. the period for which the personal data will be stored, or how that period will be calculated;
    b. the individual's right of right of access to, and rectification or erasure of the data;
    c. where processing is based on the individual's consent, their right to withdraw consent for processing their data;
    d. the individual's right to lodge a complaint with a supervisory authority;
    e. whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract (and the possible consequences of failure to provide the data);
    f. where applicable, the existence of automated decision-making;
    g. any further processing of the data that is intended for any other purpose.
3. If we receive personal data about a data subject from other sources, we must provide the data subject with the information at 7.1 and 7.2 above (as soon as possible and at the latest within one month) together with:
    a. the categories of personal data concerned; and
    b. the source from which the personal data originated, and if applicable, whether it came from publicly accessible sources.
4. The information provision requirements at 7.1 and 7.2 above will not apply where the data subject already has the information, or the provision of such information proves impossible or would involve a disproportionate effort, in which case we must take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available.

8.0 RIGHTS OF DATA SUBJECTS

1. Data subjects have certain enforceable rights under the Data Protection Legislation, including the right to obtain from the controller confirmation as to whether or not personal data concerning them are being processed and, if so, access to the personal data, plus a copy of the personal data undergoing processing, as well as information as to:
    - **a.** the purposes of the processing;
    - **b.** the categories of personal data concerned;
    - **c.** the recipients or categories of recipient of the data;
    - **d.** the envisaged period for which the personal data will be stored or, if that is not possible, the criteria used to determine that period;
    - **e.** where the personal data are not collected from the data subject, any available information as to their source; and
    - **f.** where personal data are transferred to a third country, the safeguards relating to the transfer.
2. In addition, the data subject has:
    - **a.** the right ("right of rectification") to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her and (taking into account the purposes of the processing) the right to have incomplete personal data completed;
    - **b.** the right ("right of erasure") to obtain from the controller the erasure of personal data concerning him or her without undue delay, where:
    - » the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed, or
    - » the processing is based on the data subject's consent, and the data subject withdraws consent (and there is no other legal basis for processing);
    - » the processing is based on its being necessary for the legitimate interests of the data controller or a third party, and the data subject objects to the processing, unless the controller demonstrates that the processing is based on compelling legitimate grounds which override the interests, rights and freedoms of the data subject, or is for the establishment, exercise or defence of legal claims;
    - » the processing is for the purpose of direct marketing, and the data subject objects to the processing (including profiling);
    - **c.** the right ("right of restriction") to obtain from the controller restriction of processing where the data is inaccurate, unlawfully processed, no longer required except for the establishment, exercise or defence of legal claims, or pending the verification whether the legitimate grounds of the controller override those of the data subject;
    - **d.** the right ("right of portability") to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format, and to transmit the data to another controller, where the processing is based on consent or carried out by automated means;
    - **e.** the right ("right to object") to object to processing based on the controller's legitimate interests, where these are outweighed by the interests, rights and freedoms of the data subject, unless the processing is required for the establishment, exercise or defence of legal claims;
    - **f.** the right not to be subject to a decision based solely on automated processing, including profiling

9.0 MANNER OF PROCESSING

1. In order to ensure that we comply with the Data Protection Legislation, we need to implement appropriate technical and organisational measures to ensure and to be able to demonstrate compliance, and to maintain a record of our processing activities.
2. The practical implications of this include ensuring that:
    a. we only collect personal data to the extent that it is required for the specific purpose notified to the data subject;
    b. we check the accuracy of any personal data at the point of collection and at regular intervals afterwards, and take all reasonable steps to destroy or amend inaccurate or out-of-date data;
    c. we do not keep personal data longer than is necessary for the purpose or purposes for which they were collected, and take all reasonable steps to destroy, or erase from our systems, all data which is no longer required;
    d. we process all personal data in line with data subjects' rights.
3. In addition, we will:
    a. adopt appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement the data protection principles, including data minimisation;
    b. implement appropriate technical and organisational measures to ensure that, by default, only personal data which are necessary for each specific purpose of the processing are processed ("protection by design and by default"); and
    c. where processing (in particular, when using new technologies) is likely to result in a high risk to the rights and freedoms of individuals, carry out an impact assessment of the data processing implications prior to the processing and, where necessary, consult the supervisory authority (the Information Commissioner's Office).
4. Where processing is to be carried out on our behalf by a data processor:
    a. we must ensure that the processor provides sufficient guarantees to implement appropriate technical and organisational measures so that processing meets the requirements of the Data Protection Legislation and ensures the protection of the rights of the data subjects; and
    b. processing is governed by a written contract that sets out (amongst other things) 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 our organisation as data controller.

10.0 DATA SECURITY

1. We will take appropriate security measures against unauthorised or unlawful processing of personal data, and against the accidental loss of, destruction or damage to, personal data, using appropriate technical or organisational measures.
2. We 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 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 data if they need it for authorised purposes. Personal data should therefore be stored on the company's central computer system instead of individual PCs.

3. Security procedures include:
    a. Entry controls. Any stranger seen in entry-controlled areas should be reported.
    b. Secure lockable desks and cupboards. Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)
    c. Methods of disposal. Paper documents should be shredded. Digital storage devices should be physically destroyed when they are no longer required.
    d. 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.
    e. Passwords. These must not be shared or disclosed to anyone else.
    f. Encryption. This should be used wherever it is available and appropriate.
    g. Back-ups. Regular back-ups must be taken of the information on the computer system and kept in a separate place, so that if you lose your computers, you don't lose the information.
4. Any actual or suspected breach of data security, or of this policy, must be reported to the Data Controller immediately. Data breaches will be handled in line with our data breach policy

11.0 TRANSFERRING PERSONAL DATA TO A COUNTRY OUTSIDE THE EEA

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 (this includes countries in respect of which a finding of adequacy has been made, and also transfers to entities in the USA that participate in the US-EU Privacy Shield).
    b. The data subject has explicitly consented to the transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards.
    c. The transfer is necessary for one of the reasons set out in the Data Protection Legislation, 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.
    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. This may include what are known as "binding corporate rules", or where standard data protection clauses in an approved form have been adopted.
2. Subject to the requirements in clause 10.1 above, personal data we hold may also be processed by staff operating outside the EEA who work for us or for one of our suppliers. That staff maybe engaged in, among other things, the fulfilment of contracts with the data subject, the processing of payment details and the provision of support services.

12.0 DISCLOSURE AND SHARING OF PERSONAL INFORMATION

1. We may share personal data we hold with any member of our group, which means our subsidiaries, our ultimate holding company and its subsidiaries, as defined in section 1159 of the UK Companies Act 2006, where this is necessary for certain reasons, or we have legitimate interest in doing so which are not outweighed by the interests, rights and freedoms of the data subject.
2. We may also disclose personal data we hold to third parties, on the basis of our legitimate interests:
    a. in the event that we sell or buy any business or assets, in which case we may disclose personal data we hold to the prospective seller or buyer of such business or assets; or
    b. if we or substantially all of our assets are acquired by a third party, in which case personal data we hold will be one of the transferred assets; or
    c. if we are under a duty to disclose or share a data subject's personal data in order to comply with any legal obligation, or in order to enforce or apply any contract with the data subject or other agreements; 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.

13.0 DEALING WITH SUBJECT ACCESS REQUESTS

1. Data subjects must make a formal request for information we hold about them. This must be made in writing. Employees who receive a written request should forward it to the HR Director immediately. Under the GDPR, we must usually provide information pursuant to a subject access request free of charge and within one month of the request.
2. When receiving telephone enquiries, we will only disclose personal data we hold on our systems if the following conditions are met:
    a. We will check the caller's identity to make sure that information is only given to a person who is entitled to it.
    b. We will suggest that the caller put their request in writing if we are not sure about the caller's identity and where their identity cannot be checked.
3. Our employees will refer a request to the HR Director assistance in difficult situations. Employees should not be bullied into disclosing personal information.

14.0 CHANGES TO THIS POLICY

We reserve the right to change this policy at any time. Where appropriate, we will notify data subjects of those changes

Lesley Hammond, HR & Finance Director
May 2018
8build Limited