Bespoke Project Design Ltd – GDPR Policy

This policy is not contractual but sets out the way in which we plan to manage such issues.

Introduction

Bespoke Project Design Ltd aims to conduct its business always with the highest standards of integrity and honesty. We expect all Data Subjects and workers to maintain the same standards in everything they do. All those who work for us are therefore strongly encouraged to report any perceived wrongdoing by the business or its Data Subjects, workers, contractors or agents that falls short of these principles.

Scope of this policy

This policy covers all Data Subjects (employees) and workers, including those on fixed-term contracts, any contractors, agents, casual workers or agency workers.

Note that the scope of this policy does not cover any potential breaches of a Data Subject's employment contract: these should be raised under our grievance procedure.

All employees, agents, contractors and other parties working on behalf of the organisation will be made fully aware of this policy and will be provided with a copy.

Aims of this policy

The aim of the policy is to set out our duties and responsibilities in respect of personal data as covered by EU Regulation 2016/679 General Data Protection Regulation (GDPR). The GDPR defines "personal data" as any information relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

Responsibility

The overall responsibility for implementing and monitoring the effectiveness of this policy rests with the senior management of <NAME>. The controller shall be responsible for, and be able to demonstrate, compliance with the principles.

Agents, contractors or other parties working on behalf of the organisation handling personal data will be required to indemnify the organisation and hold it harmless against any costs, liability, damages, losses, claims or proceedings that may arise out of their failure.

Training and Supervision

All employees, agents, contractors and others handling personal data will receive appropriate training and supervision including the need for care, caution, discretion and confidentiality when handling personal data. The principles of the GDPR will be made clear to them.

The performance of parties handling personal data will be reviewed regularly.

Accountability

Our Data Protection Officer is: James Needham, info@bespokeprojectdesign.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.

Data Protection Principles

The GDPR sets out the following principles with which we must comply as appropriate:

a) Must be processed lawfully, fairly and in a transparent manner in relation to Data Subjects.

b) Must collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

c) Must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

d) Must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

e) Must be 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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of Data Subjects.

Must be 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.

The rights of Data Subject s concerning personal data

The GDPR gives Data Subjects and other Data Subjects for whom we hold data the following rights to which we will adhere:

- 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

Objections to Personal Data Processing

Individuals have the right to object to:

- Processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling)
- Direct marketing (including profiling)
- Processing for purposes of scientific/historical research and statistics

We will stop processing the personal data unless:

- We can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or
- The processing is for the establishment, exercise or defence of legal claims

We will inform individuals of their right to object "at the point of first communication" and in our privacy notice.

We will stop processing personal data for direct marketing purposes as soon as we receive an objection. We will deal with an objection to processing for direct marketing at any time and free of charge.

We will inform individuals of their right to object "at the point of first communication" and in our privacy notice. This will be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.

Individuals must have grounds relating to his or her particular situation in order to exercise their right to object to processing for research purposes.

Where we are conducting research where the processing of personal data is necessary for the performance of a public interest task, we are not required to comply with an objection to the processing.

If our processing activities fall into any of the above categories and are carried out online, then we will offer a way for individuals to object online.

Why we need to collect and record Data Subject's personal data

We to keep and process information about you for normal employment purposes.

Our methods of collecting, holding and processing personal data will be regularly reviewed and evaluated.

The information we hold, and process will be used for management and administrative use only unless otherwise expressly agreed by the Data Subject.

We collect and retain this information to enable us to run the business and manage our relationship with you effectively, lawfully and appropriately, during the recruitment process, whilst you are working for us, at the time when your employment ends and after you have left.

This includes using information to enable us to provide you with the employment contract to which you are legally entitled, to comply with any other legal requirements and to pursue the legitimate interests of the Company; including protecting our legal position in the event of legal proceedings.

We will normally seek your consent to the processing of your personal data for one or more specific purposes.

If you do not provide this data, we may be unable in some circumstances to comply with our obligations and there may be implications of that decision. However, there are circumstances where your consent is not required if it's necessary to:

- Fulfil our obligations under an employment contract. This also includes steps taken at your request before entering into a contract.
- Comply with a legal obligation where we are required by UK or EU law to process the data for a particular purpose.
- Protect vital interests. We can process personal data if it's necessary to protect someone's life. This could be the life of the data subject or someone else.
- Satisfy a public task; if we need to process personal data to carry out our official functions or a task in the public interest and we have a legal basis for the processing under UK law.
- Satisfy legitimate interests; we can process personal data without consent if we have a genuine and legitimate reason (including commercial benefit), unless this is outweighed by harm to the Data Subject's rights and interests.

We will inform the Data Subject when data has been collected and processed under the above conditions.

Sensitive Personal Data

Examples of sensitive personal data are data concerning the data subject's race, ethnicity, politics, religion, trade union membership, genetics, biometrics (if used for ID purposes), health, sex life, or sexual orientation)

In order to collect and process such data we must ensure that at least one of the conditions have been met:

a) The Data Subject whom the sensitive personal data is about has given explicit consent to the processing

b) The processing is necessary so that you can comply with employment law

c) The processing is necessary to protect the vital interests of:

- the Data Subject (in a case where the Data Subject 's consent cannot be given or reasonably obtained)
- another person (in a case where the Data Subject 's consent has been unreasonably withheld)

d) The processing is carried out by a not-for-profit organisation and does not involve disclosing personal data to a third party, unless the Data Subject consents. Extra limitations apply to this condition.

e) The Data Subject has deliberately made the information public.

f) The processing is necessary in relation to legal proceedings; for obtaining legal advice; or otherwise for establishing, exercising or defending legal rights.

g) The processing is necessary for administering justice, or for exercising statutory or governmental functions.

h) The processing is necessary for medical purposes and is undertaken by a health professional or by someone who is subject to an equivalent duty of confidentiality.

i) The processing is necessary for monitoring equality of opportunity, and is carried out with appropriate safeguards for the rights of Data Subjects.

We collect and process the personal data set out in section <NUMBER> of this policy and only collect, process and hold personal data for the specific purposes set out in section <NUMBER> of this policy (or for other purposes expressly permitted by the GDPR).

Keeping Data Subjects Informed

- This document will detail the purpose(s) for which personal data is being collected and processed and the legal basis for that collection and processing
- We will keep Data Subjects covered by this policy informed at all times of the purposes for which we use personal data, including at the time of the data collection
- We will inform the data subject about data we collect from or transfer to a third party (before its transfer), including outside of the European Economic Area and its purpose
- We will only collect and process personal data for and to the extent necessary for the specific purpose or purposes of which Data Subject s have been informed (or will be informed) as set out in section One and the periods for which the data is stored
- Information supplied to data subjects concerning their data will be supplied as soon as reasonably possible and, in any event, no more than one month after the data is obtained
- This policy will detail the subjects right to withdraw their consent to the organisations processing of their personal data and their right to complain to the ICO

- Where applicable, we will inform the data subject of 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 it

- We will detail to the data subject 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

Accuracy and maintenance of Data

We shall ensure that all personal data collected, processed and held is kept accurate and up to date and will require Data Subject s for whom we maintain data to inform is of any changes as they occur.

We will check the accuracy of personal data when it is collected and otherwise as required and will take all reasonable steps to amend or erase data as appropriate.

Data will not be kept for longer than necessary as indicated by the purpose or purposes for which it was originally collected. When no longer required we will take all reasonable steps to erase or otherwise dispose of such data.

Data retention periods are covered by our Data Retention Policy.

Security of Data

Considering the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, we shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

a) The pseudonymisation and encryption of personal data

b) The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services

c) The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

d) A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing

e) In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed

f) We shall take steps to ensure that any person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by EU or UK law

g) Personal data will not be shared informally and if any person requires access to personal data then formal consent will be required from the Data Controller

h) No personal data will be transferred to employees, agents or contractors or any other parties without authorisation of the Data Controller

i) Personal data must be handled with care at all times and not left unattended or in view of other unauthorised parties

j) Leaving personal data open on a computer screen unattended is a disciplinary matter

IT Security

<SEE OUR IT POLICY>

Transfer of Personal data

The organisation will ensure the following when transferring and communicating personal data:

Emails containing personal data: All such emails will be encrypted, marked confidential and deleted once personal data has been extracted.

Wireless and Networks: Wireless networks will not be used to transfer personal data where there is a more secure alternative.

Hardcopy transfer: Hardcopy communication of personal data will be sent by secured means (e.g. sealed container by courier) and, if faxed we will ensure that the recipient is on hand to remove the communication from the machine immediately it is received.

Transferring large volumes of personal data: When it is necessary to transfer a large volume of personal data from one location to another we will use a physical disc such as a CD or DVD that will be encrypted.

A recorded delivery method or specialist courier will always be used.

Transfers to countries outside of the EEA: We do not transfer personal data outside of the EEA.

Record Keeping

We shall keep written internal records of all personal data collection, holding, and processing, including the following:

a) The name and details of the organisation, its Data Protection Officer, and any applicable third-party data processors
b) The purpose or purposes for which the Company collects, holds, and processes personal data
c) 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
d) Details of any transfers of personal data to non-EEA countries including all mechanisms and security safeguards

e) Details of how long personal data will be retained by the Company
f) Detailed descriptions of all technical and organisational measures taken by the Company to ensure the security of personal data

Storage and Disposal of Personal data

The organisation will ensure that personal data is stored safely and securely:

- Personal data will not be stored on transportable devices such as mobile phones, memory sticks, laptops etc.
- Personal data files held electronically will be backed up and encrypted by the following methods <INSERT>. Access to electronic personal data files will be restricted to employees specified by the Data Controller and by use of regularly updated passwords
- Personal data stored on hardcopy files will be stored in a locked box and cabinet at all times when not being accessed by authorised personnel
- Personal data erased or disposed of for any reason must be securely disposed of all hard copies securely shredded

Data Protection Impact Assessments

A data protection impact assessment (DPIA) is a process to help us identify and minimise the data protection risks of a project.

We must do a DPIA for certain listed types of processing, or any other processing that is likely to result in a high risk to Data Subject s' interests. We will use the Information Commissioners Office (ICO) screening checklist to help decide when to do a DPIA.

We will do a DPIA for any other major project which requires the processing of personal data.

Our DPIA will:

- Describe the nature, scope, context and purposes of the processing
- Assess necessity, proportionality and compliance measures
- Identify and assess risks to Data Subjects
- Identify any additional measures to mitigate those risks

To assess the level of risk, we will consider both the likelihood and the severity of any impact on Data Subjects. High risk could result from either a high probability of some harm, or a lower possibility of serious harm.

We will consult, where appropriate, Data Subject s and relevant experts.

If we identify a high risk and cannot mitigate that risk, we will consult the ICO before starting the processing.

Data Subjects access to personal Data

Data subjects may make a request at any time to find out what data the organisation holds about them, what has done with their personal data and why.

In order to do so they must complete a Subject Access Request (SAR) form and send it to the organisations Data Protection Officer (DPO) named in this policy.

The DPO must respond within one month of receipt or may inform the data subject making the request that he wishes to extend it to two months if the SAR is complex and/or numerous requests have been made.

No fee will be charged for such requests unless the requests are repetitive and/or unfounded or excessive.

Rectification of personal Data

Under Article 16 of the GDPR Data Subject s have the right to have inaccurate personal data rectified. A Data Subject may also be able to have incomplete personal data completed – although this will depend on the purposes for the processing. This may involve providing a supplementary statement to the incomplete data.

If we receive a request for rectification we will take reasonable steps to satisfy ourselves that the data is accurate and to rectify the data if necessary. We will take into account the arguments and evidence provided by the data subject.

What steps are reasonable will depend, in particular, on the nature of the personal data and what it will be used for.

As a matter of good practice, we may restrict the processing of the personal data in question whilst we are verifying its accuracy, whether or not the Data Subject has exercised their right to restriction.

We will let the Data Subject know if we are satisfied that the personal data is accurate and tell them that we will not be amending the data. We will explain our decision and inform them of their right to make a complaint to the ICO or another supervisory authority; and their ability to seek to enforce their rights through a judicial remedy.

We will place a note on the system indicating that the Data Subject challenges the accuracy of the data and their reasons for doing so.

We can refuse to comply with a request for rectification if the request is manifestly unfounded or excessive, taking into account whether the request is repetitive in nature. Alternatively, we may request a "reasonable fee" to deal with the request.

We will justify our decision and inform the data subject making the request within one month making them aware of their right to make a complaint to the ICO or another supervisory authority; and their ability to seek to enforce this right through a judicial remedy.

Data subjects should make requests for rectification in writing direct to the organisations Data Protection Officer.

If changes are made following a request for rectification we will notify other bodies holding the same data and inform the data subject accordingly.

Erasure of Personal Data

The data subject has the right to request the erasure of any of their personal data in certain circumstances:

- The personal data is no longer necessary for the purpose which it was originally collected or processed for
- If we are relying on consent as our lawful basis for holding the data, and the individual withdraws their consent
- If we are relying on legitimate interests as our basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing
- If we are processing the personal data for direct marketing purposes and the individual objects to that processing
- If we have processed the personal data unlawfully (i.e. in breach of the lawfulness requirement of the 1st principle)
- If we have to do it to comply with a legal obligation
- If we have processed the personal data to offer information society services to a child

The right to erasure does not apply in the following circumstances:

The right to erasure does not apply if processing is necessary for one of the following reasons:

- To exercise the right of freedom of expression and information
- To comply with a legal obligation
- For the performance of a task carried out in the public interest or in the exercise of official authority
- For archiving purposes in the public interest, scientific research historical research or statistical purposes where erasure is likely to render impossible or seriously impair the achievement of that processing
- For the establishment, exercise or defence of legal claims

We will act upon the request without undue delay and at the latest within one month of receipt.

We can extend the time to respond by a further two months if the request is complex or we have received a number of requests from the individual. We will let the individual know without undue delay and within one month of receiving their request and explain why the extension is necessary.

If we decide that there is not good reason to erase the data, we will tell them that we will not be erasing the data. We will explain our decision and inform them of their right to make a complaint to the ICO or another supervisory authority; and their ability to seek to enforce their rights through a judicial remedy.

We will place a note on the system indicating that the Data Subject has requested erasure and their reasons for doing so.

We can refuse to comply with a request for erasure if the request is manifestly unfounded or excessive, taking into account whether the request is repetitive in nature. Alternatively, we may request a "reasonable fee" to deal with the request.

We will justify our decision and inform the data subject making the request within one month making them aware of their right to make a complaint to the ICO or another supervisory authority; and their ability to seek to enforce this right through a judicial remedy.

Data subjects should make requests for erasure in writing direct to the organisations Data Protection Officer.

If erasure takes place, we will notify other bodies holding the same data and inform the data subject accordingly.

Restriction of Personal Data Processing

The data subject has the right to obtain from the data controller restriction of processing where one of the following applies:

- The accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data
- The processing is unlawful, and the data subject opposes the erasure of the personal data and requests the restriction of their use instead
- The controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims
- The data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject

Where processing has been restricted such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the EU or the UK.

A data subject who has obtained restriction of processing shall be informed by the controller before the restriction of processing is lifted.

Data Portability

Data subjects are entitled to obtain and reuse their personal data for their own purposes across different services.

It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

The right to data portability only applies:

- To personal data an individual has provided to a controller
- Where the processing is based on the individual's consent or for the performance of a contract
- When processing is carried out by automated means

The organisation processes personal data using various automated means <INSERT DETAILS>.

We will provide the personal data in a structured, commonly used and machine-readable form. The information will be provided free of charge.

If the individual requests us to transmit the data directly to another organisation we will do so if this is technically feasible. However, we are not required to adopt or maintain processing systems that are technically compatible with other organisations.

We will respond to such requests without undue delay, and within one month.

This can be extended by two months where the request is complex, or we receive a number of requests. You will inform the individual within one month of the receipt of the request and explain why the extension is necessary.

Where we are not taking action in response to a request, we will explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy without undue delay and at the latest within one month.

Data Breaches

A breach can have a range of adverse effects on individuals, which include emotional distress, and physical and material damage. Some personal data breaches will not lead to risks beyond possible inconvenience to those who need the data to do their job. Other breaches can significantly affect individuals whose personal data has been compromised. We will assess this case by case, looking at all relevant factors.

When a personal data breach has occurred, the Data Protection Officer must be informed immediately.

He will establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it's likely that there will be a risk, then he will notify the ICO within 72 hours; if it's unlikely then we will not report it. However, if we decide we don't need to report the breach, we will document it.

Where we use a data processor, and this processor suffers a breach, then under Article 33(2) it must inform us without undue delay as soon as it becomes aware. We will make any such processors aware of this responsibility.

Implementation, monitoring and review of this policy

This policy will take effect from <DATE>. The Directors have overall responsibility for implementing and monitoring this policy, which will be reviewed on a regular basis following its implementation and may be changed from time to time.

Signed: *J Needham*

James Needham - Director

Date: 14th December 2020