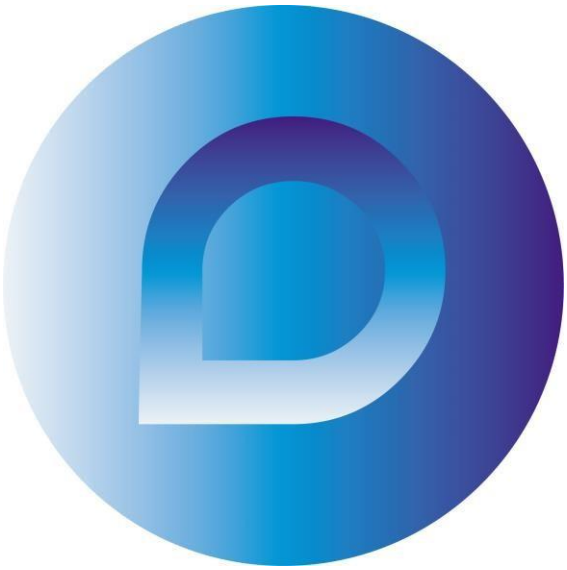
European Union
European
Social Fund

part funded by European Social Fund (ESF)
and Youth Employment Initiative (YEI)

bydesign

Data Protection Policy & Procedures



Revised: 18th December, 2019 **Next Review By: 17th December, 2020**

bydesign

By Design Group Ltd, 49 Kepler, Lichfield Road Ind. Est., Tamworth, Staffordshire, B79 7XE.
Tel: 01827 316297 Fax: 01827 723889 Web: www.bydesign-group.co.uk

Data Protection Policy and Procedures

Introduction

On May 25, 2018, a new landmark privacy law called the General Data Protection Regulation (GDPR) took effect in the European Union (EU). The GDPR expands the privacy rights granted to individuals, and it places obligations that handle personal data. By Design Group takes its responsibilities with regard to the management of the requirements of GDPR very seriously. This policy sets out how the organisation manages those responsibilities.

Statement of Policy

In order to operate efficiently, By Design Group and associated companies has to collect and use information about people with whom it works with. These may include members of the public, current, past and prospective employees and volunteers, clients and customers, and suppliers. This personal information must be handled and dealt with properly, however it is collected, recorded and used, and whether it be on paper, in computer records or recorded by any other means, there are safeguards within the Regulation to ensure this.

By Design Group and related companies regard the lawful and correct treatment of personal information as very important to its successful operations and to maintaining confidence between the organisation(s) and those with whom it carries out business. The company will ensure that it treats personal information lawfully and correctly.

To this end the company fully endorses and adheres to the Principles of General Data Protection Regulation (GDPR).

The Principles of GDPR

The regulation stipulates that anyone processing personal data must comply with all **Six Principles** of following principles.

These Principles are legally enforceable and require that personal information:

1. Shall be processed fairly, lawfully and in a transparent manner. Personal data shall not be processed unless specific conditions are met;
2. Shall be obtained only for one or more specified, explicit and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes;
3. Shall be adequate, relevant and limited to what is necessary, in relation to the purpose or purposes for which it is processed;
4. Shall be accurate and where necessary, kept up to date. Inaccurate personal data should be corrected or deleted;
5. Shall not be kept for no longer than is necessary for that purpose or those purposes;
6. Shall be kept secure i.e. protected by an appropriate degree of security;

Conditions of Processing Personal Data

Under the regulations, the processing of personal data will only be lawful if it satisfies at least one of the following processing conditions:

1. Data subject has unambiguously given their consent to processing their data for one or more specific purposes.

And or, processing is necessary for the:

2. Performance of a contract with the individual;
3. Compliance with a legal obligation to which the controller is subject to.
4. Protection of the individual's vital interests or of another identifiable person.
5. Performance of a task carried out in the public interest.
6. Purposes of the legitimate interests pursued by the controller or processor, as long as these interests do **not** override the interests or fundamental rights of the data subject.

The Regulation provides conditions for the processing of any personal data. It also makes a distinction between personal data and 'special categories' of data.

Personal data is defined as information relating to an identified or identifiable natural person who can be recognised from:

- That information.
- That data and other information which in the possession of, or is likely to come into the possession of the data controller and includes an expression of opinion about the individual and any indication of the intentions of the data controller, or any other person in respect of the individual.

Special categories of personal data is defined as personal data consisting of information as to:

- Racial or ethnic origin.
- Political opinion.
- Religious or other beliefs.
- Trade union membership.
- Processing of generic data.
- Physical or mental health conditions.
- Sexual orientation.
- Biometric and genetic data

Conditions of Processing Special Categories of Data

The Regulation places much stronger controls on the processing of special categories of personal data. Processing that reveals any special categories of data, for the purpose of uniquely identifying a natural person is prohibited.

Unless one or more of the following applies:

1. The individual has given explicit consent for this processing.
2. Personal data which is manifestly made public by the data subject. i.e. on website

And/ or processing is necessary to:

3. Fulfil legal obligation in the field of employment and social security law.
4. Protect the vital interests of the individual or of another natural person.
5. Perform legitimate activities of a not-for-profit body and only relates to members or related persons and the personal data is not disclosed outside that body without consent;
6. Establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
7. Reasons of substantial public interest.
8. Healthcare purposes and is subject to suitable safeguards;

9. Public health purposes and is based on Union or Member State law; or
10. Archiving, scientific or historical research purposes or statistical purposes and is based on Union or Member State law.

Under regulations, the processing of criminal offences and convictions is strictly prohibited. There are no justifications; even consent from individual will not justify the processing of this type of data, unless the Information Commissioners Office (ICO) or UK law authorises it.

Handling of Personal / Sensitive Information

By Design Group and associated companies will, through appropriate management and the use of strict criteria and controls:

- Observe fully conditions regarding the fair collection and use of personal information.
- Take measures to provide any information that regulation demands, in a concise, transparent, intelligible and easily accessible form, using plain language; particularly when addressing a child.
- Meet its legal obligations to specify the purpose for which information is used.
- Collect and process appropriate information and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements.
- Ensure the quality of information used.
- Apply strict checks to determine the length of time information is held.
- Take appropriate technical and organisational security measures to safeguard personal information.
- Ensure that personal information is not transferred abroad without suitable safeguards.
- To act on and facilitate any requests of the data subject for exercising his or her rights, within the statutory 28 days.

These include:

- The right to be informed of the relevant information under this Regulation, relating to the processing of one's personal data.
- The right of access to one's personal information.
- The right to prevent, restrict, object to processing in certain circumstances.
- The right to correct, rectify, block or erase information regarded as wrong information.
- The right to erase any information concerning him or her.
- The right to request the transfer of personal data to another controller, when the legal basis for processing is consent.
- The right to object to automated individual decision-making.

In addition, we will endeavour to ensure that:

- There is someone with specific responsibility for data protection in the organisation.
- Everyone managing and handling personal information understands that they are contractually responsible for following good data protection practice.
- Everyone managing and handling personal information is appropriately trained to do so.
- Everyone managing and handling personal information is appropriately supervised.
- Anyone wanting to make enquiries about handling personal information, whether a member of staff or a member of the public, knows what to do.
- Queries about handling personal information are promptly and courteously dealt with.
- Methods of handling personal information are regularly assessed and evaluated.
- Performance with handling personal information is regularly assessed and evaluated.
- Data sharing is carried out under a written agreement, setting out the scope and limits of the sharing.
- Any disclosure of personal data will be in compliance with approved procedures.

All relevant employees are to be made fully aware of this policy and of their duties and responsibilities under the regulation.

All employees working for company will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure and in particular will ensure that:

- Paper files and other records or documents containing personal / special categories of data are kept in a secure environment.

  The vast majority and wherever possible, personal data held on computers and computer systems will be stored within the company's server or on our cloud-based Customer Relationship Management (CRM) solution. Any documents containing personal data, stored outside the server and CRM solution, will be protected by the use of a password; which where possible have forced changes periodically.

- Individual passwords should be such that they are not easily compromised.

All contractors, consultants or other partners must:

- Ensure that they and all of their staff who have access to personal data held or processed for or on behalf of the company, are aware of this policy and are fully trained in and are aware of their duties and responsibilities under the Regulation. Any breach of any provision of the Regulation will be deemed as being a breach of any contract between the company and that individual, company, partner or firm.
- Allow data protection audits by the company of data held on its behalf (if relevant and requested).
- Indemnify the company against any prosecutions, claims, proceedings, actions or payments of compensation or damages, without limitation where relevant.

All contractors who are users of personal information supplied by the company will be required to confirm that they will abide by the requirements of the Regulation with regard to information supplied by the company.

Data Protection Impact Assessment:

GDPR requires a Data Protection Impact Assessment (DPIA) to be completed when processing is likely to result in a high risk to the rights and freedoms of individuals; as it identifies and helps minimise the data protection risks of a project or plan.

GDPR defines "high risk" as either harm is more likely to occur or because the potential harm is more severe, or a combination of the two. If no measures can be taken to avoid or reduce this risk, consultation with ICO must take place, before processing can begin.

DPIA is automatically required when the following processing occurs:

- Systematic and extensive profiling with significant effects.
- Large scale of special categories of data.
- Public monitoring.

Information Commissioners Office (ICO) has also published a list that includes, but is not limited to examples of processing operations that require a DPIA:

- Use of new technologies
- A denial of an individual's access to a product, service or opportunity
- Profiling of any individuals on a large scale
- Any information relating to biometric data

- Any information relating to genetic data, other than by an individual GP or health professional.
- Combining, comparing or matching of personal data
- Personal data that has not been obtained directly from data subject.
- Involves the tracking of an individual's geolocation or behaviour. i.e. online environment
- Using personal data of children or vulnerable individuals for marketing purposes, profiling or other automate decision-making.
- The nature of processing could jeopardise the physical health or safety of individual(s)

Exceptions: DPIA isn't needed under the following circumstances:

- There is a clear statutory basis for processing
- The legal provision or a statutory code specifically provides for and regulated the processing operation in question
- DPIA is not required subject to other obligations
- A data protection risk assessment was carried out as part of the impact assessment when the legislation was adopted.
- A DPIA of a similar nature has already been carried out.

If a Data Protection Impact Assessment is required, this will be overseen by our Data Protection Officer (DPO) and undertaken on the relevant Information Commissioner Office DPIA recommended template:

https://ico.org.uk/media/about-the-ico/consultations/2258461/dpia-template-v04-post-comms-review-20180308.pdf

Data Breach Procedure

The Regulation defines a personal data breach as the accidental or unlawful destruction, unauthorised disclosure of or loss of information relating to an identifiable person.

All employees must inform their supervisor and Data Protection Officer (DPO) immediately about a data breach or violations against this Data Protection Policy.

Any employee, volunteer, partner, or data subject may approach the DPO, at any time to raise concerns, ask questions, request information or make complaints relating to data protection or data security issues.

Contact details of DPO are as follows: Geoff Parsons (01827 316297 & geoffparsons@bydesign-group.co.uk)

Oversight

The company has appointed Geoff Parsons as the companies Data Protection Officer (DPO). He will be responsible for ensuring that the Policy is implemented and adhered to and will include:

- Advising staff, employees, and contractors of its legal obligations. The provision of cascade data protection training, for staff within the company, if appropriate.
- For the development of best practice guidelines.
- For carrying out compliance checks to ensure adherence with the Data Protection Regulation.

Notification to the Information Commissioner Office

The Information Commissioners Office maintains a public register of data controllers. By Design Group is registered as such, Registration Number: Z4558005 currently until 28 February 2022 - renewed annually.

The General Data Protection Regulation requires every data controller who is processing personal data, to notify and renew their notification, on an annual basis. Failure to do so is a criminal offence. By Design Group will review the Data Protection Register at least annually, prior to notification to the Information Commissioner.

Any changes to the register must be notified to the Information Commissioner, within 28 days. To this end, any changes made between annual reviews will be brought to the attention of the Office Manager (Information Officer) immediately and then notified accordingly.

Cyber Essentials Plus Accreditation

As part of the companies ongoing commitment to Data Protection and GDPR the company was awarded the Cyber Essentials Plus accreditation.

Date of Certification: 25th November 2019
Recertification Due: Nov 2020
Certificate Number: IASME-A-014344