Data Protection Policy

1. GENERAL

1.1. Designer Group complies with all legal requirements applying to control, processing and protection of employees' personal data. The company is fully compliant with all provisions of current Data Protection legislation.

1.2 Full details of employee data processing activities are contained in the company's Data Protection and Privacy Notice, a copy of which can be accessed on DG Hub and on Designer Group's website.

1.3 We process employees' data in order to fulfil our contractual obligations to our employees and to comply with our common law and statutory obligations.

1.4 From time to time we may also ask for your agreement to complete feedback questionnaires and to provide information about your experience and qualifications to clients and prospective clients as part of the pre-qualification process.

1.5. We hold and process data in order to:

- administer and maintain personnel records;
- pay and review salary and other remuneration benefits;
- provide and administer benefits (including if relevant, pension, life insurance, permanent health insurance and medical insurance);
- undertake performance appraisals and reviews;
- maintain sickness and other absence records;
- take decisions regarding fitness for work;
- provide references and information to future employers;
- provide information to governmental and quasi-governmental bodies for tax, Social Insurance, social security and other purposes;
- provide information to future purchasers of the company and to prospective transferees of any part of the business.

2. EMPLOYER OBLIGATIONS

2.1 Designer Group complies with all appropriate data protection principles. We will therefore:

- process data lawfully, fairly and in a transparent manner and process it for only specified and lawful purposes;
- ensure that all data obtained is adequate and relevant to those lawful purposes and is accurate, up to date and kept no longer than necessary;
- process all data in accordance with each employee's statutory rights;
- take the appropriate security measures to protect the data from unauthorised disclosures.

3. RESPONSIBILITIES OF DATA USERS

3.1. Key points

3.1.1 Collection and management of employee data

Staff who process employees' personal data have a duty to ensure that information is only collected for its stated purpose, that it is factual and that information is kept securely and destroyed in accordance with company and statutory regulations.

All members of staff who have access to other staff members' personal data as part of their job must at all times ensure that:

- Information is used only for the purpose(s) for which it was collected;
- data confidentiality is maintained at all times;
- data accuracy is maintained;
- data is held securely;
- only data necessary for the conduct of normal company business is retained;
- confidential data, whether held in paper format or electronically, is destroyed when no longer required.

3.1.2 Disclosure of employees' personal data

Employees' information should not be disclosed to anyone without proper authority. Staff should contact the Human Resources Manager if they have any questions regarding disclosure of personal data. Any employee who discloses another individual's personal data without proper authorisation may be subject to disciplinary proceedings.

3.1.3 Internal disclosure

Personal information should only be disclosed to other members of Designer Group's staff if the staff member concerned has given permission or if the disclosure is necessary for the legitimate interests of the company. Personal information must not be disclosed merely for social reasons.

3.1.4 External disclosure

Generally, personal data should not be given out externally, except where there is a legal or contractual requirement to do so, without the permission of the staff member concerned. It is permissible to provide personal data in emergency situations, (i.e. where the individual's or someone else's life may be in danger).

Personal data should not be disclosed over the telephone unless you are certain of the identity of the caller and that you are authorised to release the information. Requests for information from the Gardai or other investigatory bodies should be directed to the Human Resources Manager.

Another reason for us to disclose personal data would be to adhere to pre-tender qualification requests for clients. This would include company CV, business photo, career history and training records. The information submitted would only be used for a legitimate business reason specifically in relation to a tender.

3.1.5 Reporting a Data Breach

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Examples can include:

- access by an unauthorised third party;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission; and
- loss of availability of personal data.

If you become aware of a personal data breach, you must report this to Fiona Ebbs, HR Administration, without delay.

4. EMPLOYEE'S RIGHTS

4.1. The Right to be Informed

Our Data Protection and Privacy Notice provides a description of the personal data being processed; and the persons or classes of persons to whom the data may be disclosed, together with details of associated policies and safeguards.

4.2 Right of Access

On making a written request, employees have the right to be told the content of the personal data relating to themselves and being processed by the company. This information will be provided within one month of receiving such a request.

4.3 Correction of Inaccurate Data

If, on viewing that personal data processed by ourselves, an employee considers the data to be inaccurate, then he or she has the right to ask the company to amend any inaccuracies or to remove any data that is inaccurate or out of date. The employee also has the right to request the company restricts or stops processing the data. Please note that this does not apply where we are processing data in fulfilment of our legal obligations. Any such request should be made to the Human Resources Manager in writing. The company has a requirement to maintain accurate and up to date information, and for that purpose there is an obligation upon employees to keep us informed of all changes to personal data including changes of address, marital status and next of kin from time to time.

4.4 Right to Data Portability

The right to data portability applies where the employee has provided information and where processing is carried out by automated means. Where this is the case, the company will provide the personal data in a structured, commonly used and machine readable form.

If requested and where technically feasible, the company may transmit the data directly to another organisation. Any such requests will be fulfilled within one month, although this may be extended where the request is complex or where there are a number of requests.

5. FURTHER INFORMATION

5.1 Further detailed information is contained in our Data Protection and Privacy Notice and our policy on use of Company Communications Systems. If you have any questions about these policies or any other issues relating to data protection, please consult the Human Resources Manager in the first instance.