BELFRY PROPERTY SEVICES Ltd
GDPR Policy Document and Privacy Notice
General Data Protection Regulation

Background

The Managing Director of Belfry Property Services Ltd has put into effect the required elements of the Regulation and is in compliance with the 2016 General Data Protection Regulation as evidenced by this document.

The Managing Director Marc Fage, under the Regulation, has assumed the responsibility of Data Controller and has delegated the responsibility of Data Protection Officer (DPO) to the General Manager Aisling Fage.

The DPO has completed a Data Audit, which is reviewed annually, and produced a Privacy Impact Assessment and a Data Retention Policy. Belfry staff are made aware of GDPR requirements by means of this document, the Belfry Property Services Ltd GDPR Policy Document and Privacy Notice.

Key concepts

As given in the Regulation:

The GDPR

- 'lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data'.
- 'protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data'.
- 'applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.'

The GDPR does **not** apply to a purely personal or household activity.

The data protection principles

Under the GDPR the data protection requirements are underwritten by 7 principles, requiring data to be:

1. *'processed lawfully, fairly and in a transparent manner'*

   (Note: For processing to be lawful by the company, it must be carried out only for one or more of a number of lawful conditions. For more on this see Lawful Conditions for processing.)

2. *'collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes'*

3. *'adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed'*

   (Note: This principle is stricter than its predecessor under the DPA (Data Protection Act), which requires that the data held by the company is not "excessive" in relation to the purposes for which it is processed. This makes it more difficult for organisations to collect data for a general purpose.)

4. *'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 it is processed, is erased or rectified without delay.'*

   (Note: The GDPR therefore imposes an express obligation for the removal or correction of inaccurate data held by Belfry without delay'.)

5. *'kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data are processed.'*

   (Note: The GDPR includes exceptions to this principle. Of relevance to Belfry staff is the storage of personal data 'for longer periods where it is processed solely for 'statistical purposes' providing 'appropriate technical and organisational measures [to be in place] to safeguard the rights and freedoms of data subjects'.)

6. *'processed in a manner that ensures appropriate security... including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.*

   (Note: The DPO has liaised with IT and services providers to ensure suitable virus protection is applied and that applicable means are taken to prevent unauthorised access. If it is deemed necessary, some data may be encrypted to ensure safe transfer, including by SSL certificated server/s)

7. *'the controller shall be responsible for, and be able to demonstrate compliance with, [the other data protection principles]: This is referred to as Accountability.*

   (Note: Accountability has no equivalent under the DPA and is a new concept for data protection, but is covered by the current arrangements made by the company to ensure that all processing of personal data by employers must be carried out in accordance with the data protection principles at all times.)

Lawful conditions for processing

Belfry recognises that employers can only lawfully process personal data for certain limited reasons or conditions. There are 6 lawful conditions but only 4 are likely to apply to the company in the employment context. These are quoted in the GDPR as:

1. 'the data subject has given consent... for one or more specific purposes.'
2. 'the processing is necessary for the performance of a contract to which the data subject is party or... to take steps at the request of a data subject prior to entering into a contract.'
3. 'the processing is necessary to comply with a legal obligation to which the controller is subject.'

4. 'the processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests and fundamental rights and freedoms of the data subject.'

The DPO is satisfied that most, if not all, day to day legitimate uses of personal data can be lawfully done by Belfry relying on one (or more) of the lawful conditions above.

Personal data

Personal data under the Regulation is:

*'any information relating to an identified or identifiable **living** individual'.*

An identifiable living individual means 'a living individual who can be identified, directly or indirectly, in particular by reference to either of the following:

- *One or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual'*
- *An identifier such as a name, an identification number, location data or an online identifier'*

In the context of the GDPR, personal data will relate to employees, but it can also include agency workers and self-employed contractors.

Under the GDPR requirements, the DPO has carried out a data audit of how personal data is sought, used, maintained and accessed in order to comply with the GDPR needs for security, probity and appropriate use.

To comply with GDPR employees will be asked to consent officially (by means of a signed declaration) to personal information being held by the company.

Examples of personal data that Belfry Property Services Ltd will need to hold about employees include:

- Name
- Title
- Address
- Home telephone/mobile numbers
- Email address
- Date of birth
- Gender
- Marital status
- Children and dependants
- Next of kin
- Emergency contact information

- National insurance number
- Health declaration
- Driver's license number & details
- Identification card numbers including CSCS cards etc
- Bank account details
- Payroll information
- Salary, annual leave and benefits information
- Job title
- Performance information
- Location of employment
- Education
- Training (including learning difficulties or disabilities
- References
- Work history
- Proof of work eligibility (ie right to work in UK, Passport, Work Visa etc as required by DWP and Border Agency)
- Photograph for ID, other security purposes, marketing
- Employee number
- Compensation history
- Performance information
- Disciplinary and grievance information
- Pension and Insurance enrolment information

Other information under 'special categories of personal data' (see below) may apply to some employees:

Special categories of personal data

Special categories of personal data (currently known as sensitive personal data) may be necessary to be held in certain circumstances. This covers what the GDPR defines as:

'information that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life and sexual orientation and genetic or biometric data.'

The Controller and DPO consider that such information would only be held in exceptional circumstances. Express permission to process such data will be sought from the employee at the time and may include:

- Criminal conviction information
- Payments from salary to dependants
- Court awards
- Specific health issues and disability accommodation

Processing

Processing of personal data is defined as:

'an operation or set of operations which is performed on personal data or on sets of personal data... such as collection, recording, organisation, structuring or storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction'

The list is not exhaustive but covers, in general, all that Belfry may wish to do with data about its employees, whether this is done electronically or on paper.

Transfer of data and data-sharing

The DPO has determined that the transfer of certain personal data is legitimate and necessary and is passed to the following entities from time to time:

HMRC – Reference employment and taxation requirements

National Insurance – Reference employment and earnings status, also linked to benefits accrual

Payroll providers – Reference monthly payment of salary or wages

Insurers – Reference company insurance provision, including insurance for driving company vehicles

Pensions providers – Reference employee pension provision and entitlement

IT Service Providers

Medical Insurance – as applicable

HSE – reference RIDDOR reporting and accident/near-miss reporting and investigation

Court Services – ref child/beneficiary upkeep and provision or CCJs

Client/Principal Contractor – Ref security and site access, Induction training, qualifications, Card ID eg CSCS.

Belfry Property Services Ltd will not provide personal information to any other third parties for marketing, sales purposes or any other issues..

Company Retention Policy

The company will retain information or records about employees, no longer than necessary, but must also comply with current statutory requirements such as employment law, right to work status, HMRC requirements and Safety law.

The company retention of data will thus be:

Personal details, work history, contact address etc	7 Years after leaving employment
Remuneration inc overtime, bonus, expenses	7 years
Application Forms and interview notes	6 months to 1 year
Time cards	2 years after audit
Working hours	2 years after they are made
Pensioners records	12 years after end of benefit
Pension scheme investment policies	12 years from the ending of benefit payable
Parental leave	Until child is 18 (birth or adoption)
Statutory Maternity Pay inc calculations, certs, medical evidence	3 years after tax year when period ends
Redundancy details, calculations, notifications etc	6 years after date of redundancy
Occupational Safety and Health Including Assessments under H&S law & records of consultations with staff	Up to 40 years
Statutory Sick pay records, calculations, certs etc	6 after employment ceases (advised)
Photographic images	4 Years after leaving employment
Disciplinary Information	6 Years after leaving employment

The retention of information can also be of benefit to some employees and sub-contractors who may require a job reference in the future and to some employees or sub-contractors who may wish to resume employment with Belfry after leaving for a period for eg career progression, family reasons or moving to another area.

The rights of employees and data subjects

A requirement of the GDPR is that this Document and Privacy Notice is available to employees and explains employees and data subject's rights.

These are as follows - the right to:

- information (as expressed in this Policy Document & Privacy Notice)
- access to personal data
- correction of personal data
- erasure of personal data (also known as the right to be forgotten)
- restrict data processing
- object to data processing
- receive a copy of personal data or transfer it to another controller
- not be subject to automated decision-making

- be notified of a security breach

Accessing your Personal Information

Employees or data subjects (eg including possibly clients and sub-contractors) wishing to have access to their personal data, or their employees personal data, should put their request in writing (hard copy or email) to the Commercial Manager acting as the DPO. The DPO will endeavour to respond to any such written request, as soon as is reasonably practical and within 32 days to access the records and effect a disclosure. Although allowed under the regulation, the DPO will not currently make a charge for this facility.

Records of Processing

Belfry is required to maintain a record of processing activities. An assessment has been made, as part of the Data Audit, of the uses made of personal information and the transmittal and sharing of data. The overall record is produced as a table and is enclosed as an Appendix. The data will be periodically updated and at least annually.

Data Subject Images

Facial and profile images may be required for training recognition and security purposes. This may be required for eg Identity Card purposes. Additionally, from time to time, Belfry (similar to many companies) may require photographs to be taken while working for clients, or to demonstrate head office activities, as a means of marketing for brochures, presentations etc. Such photographs are likely to include staff, but will exclude those who express a wish at the time not to be included. Close-up pictures taken for corporate brochures will require express permission and a Model Release form is likely to be used.

Staff will appreciate that once images are used for marketing, it may not be possible to change layouts or extract images during the currency period of the material (up to 6 years or more), hence the probable use of a model release form.

On a number of client sites, including head office, security video cameras will be recording movements on a 24/7 basis. These are security features that are installed for the security and protection of staff and the companies involved. Images will only be used in the event of an investigation.

Requirement of Consent

A feature of the GDPR is that employees and data subjects must give consent for their data to be processed. This is important as it is seen as a lawful condition and Belfry will require all new employees to sign a consent form at the time of commencing employment. For current employees and applicable sub-contractors, a similar consent form (Total Office/OMM GDPR Employee Consent Form) will need completion.

The consent form will clearly indicate the categories of data currently held and/or required for future employment. Each category will require a box tick by the employee/data subject to expressly allow Belfry to process the data.

This follows the GDPR requirement that ***Consent*** must be:

'any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.'

Breaches of Data Security

Belfry recognises that if personal data held by Belfry is processed incorrectly it has potential to cause damage to the data subject. This could range from identity theft or fraud, financial loss, to damage to their reputation and/or loss of confidentiality.

Belfry will document any personal data protection breach, including the facts connected with the breach, its effects and remedial action taken.

The Government supervising authority will be able to inspect these records.

If Belfry believes or knows that a data breach has occurred, it is required to notify the supervising authority if the breach is likely to result in a risk to the rights and freedoms of individuals.

The notification must be made no later than 72 hours of becoming aware of the breach. Initial notification only is necessary within this time period and further information can be provided "in phases without undue delay".

Employees, likewise, will be notified without undue delay.

Signed:
Mark Fage
Managing Director

Date: 17.05.2018