Data Protection Policy

Document Description

This document outlines our legal requirements under the General Data Protection Regulations and the processes for how J&B meets them. Note: until GDPR come into force on 25 May 2018 the current Data Protection Act 2000 will continue to apply.

Implementation and Quality Assurance

Implementation is immediate and this Policy shall stay in force until any alterations are formally agreed.

The Policy will be reviewed every two years, sooner if legislation, best practice or other circumstances indicate this is necessary.

All aspects of this Policy shall be open to review at any time. If you have any comments or suggestions on the content of this policy please contact our HR Manager at J&B Recycling Ltd, Thomlinson Road, Hartlepool, TS25 1NS 01429 272810

Introduction

The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a regulation by which the European Parliament, the European Council and the European Commission intend to strengthen and unify data protection for individuals within the European Union (EU). It also addresses the export of personal data outside the EU. The primary objectives of the GDPR are to give citizens back control of their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU. When the GDPR takes effect it will replace the data protection directive (officially Directive 95/46/EC) from 1995. The regulation was adopted on 27 April 2016 and applies from 25 May 2018 after a two-year transition period.

The 1998 Data Protection Act, which came into force on 1 March 2000, will continue to apply until the new General Data Protection Regulations come into force in May 2018.

The following guidance is not a definitive statement on the Regulations, but seeks to interpret relevant points where they affect J&B.

The Regulations cover both written and computerised information and the individual's right to see such records.

It is important to note that the Regulations also cover records relating to staff and volunteers.

All J&B staff are required to follow this Data Protection Policy at all times.

The Managing Director has overall responsibility for data protection within J&B but each individual processing data is acting on the controller's behalf and therefore has a legal obligation to adhere to the Regulations.

Definitions

- Processing of information – how information is held and managed.
- Information Commissioner - formerly known as the Data Protection Commissioner.
- Notification – formerly known as Registration.
- Data Subject – used to denote an individual about whom data is held.
- Data Controller – used to denote the entity with overall responsibility for data collection and management. J&B is the Data Controller for the purposes of the Act.
- Data Processor – an individual handling or processing data
- Personal data – any information that enables a person to be identified
- Special categories of personal data – information under the Regulations that requires the individual's explicit consent for it to be held by J&B.

Data Protection Principles

As data controller, J&B is required to comply with the principles of good information handling.

These principles require the Data Controller to:

1. Process personal data fairly, lawfully and in a transparent manner.
2. Obtain personal data only for one or more specified and lawful purposes and to ensure that such data is not processed in a manner that is incompatible with the purpose or purposes for which it was obtained.
3. Ensure that personal data is adequate, relevant and not excessive for the purpose or purposes for which it is held.
4. Ensure that personal data is accurate and, where necessary, kept up-to-date.

5. Ensure that personal data is not kept for any longer than is necessary for the purpose for which it was obtained.
6. Ensure that personal data is kept secure.
7. Ensure that personal data is not transferred to a country outside the European Economic Area unless the country to which it is sent ensures an adequate level of protection for the rights (in relation to the information) of the individuals to whom the personal data relates.

Consent

J&B must record the Data Subjects explicit consent to storing certain information (known as 'personal data') on file.

For the purposes of the Regulations, personal data and special categories of personal data covers information relating to:

- The racial or ethnic origin of the Data Subject.
- His/her political opinions.
- His/her religious beliefs or other beliefs of a similar nature.
- Whether he/she is a member of a trade union.
- His/her physical or mental health or condition.
- His/her sexual life.
- The commission or alleged commission by him/her of any offence
- Online identifiers such as an IP address or email address
- Name and contact details
- Genetic and/or biometric data which can be used to identify an individual

Consent is not required to store personal that is essential to enable a Service to be provided to the customer.

As a general rule in other cases J&B will always seek consent where personal or special categories of personal information is to be held.

If personal and/or special categories of personal data need to be recorded for the purpose of service provision and the customer refuses consent, the case should be referred to the relevant J&B service manager for advice.

Obtaining Consent

Consent may be obtained in a number of ways depending on the nature of the requirement, and consent must be recorded on or maintained with the relevant records:

- face-to-face
- written
- telephone
- email

Face-to-face/written
A pro-forma should be used.

Telephone
Verbal consent should be sought and noted on the relevant record.

E-mail
The initial response should seek consent.

Consent obtained for one purpose cannot automatically be applied to all uses e.g. where consent has been obtained from a Customer in relation to information needed for the provision of a service, separate consent would be required if, for example, direct marketing of other services was to be undertaken.

Specific consent for use of any photographs and/or videos taken should be obtained in writing. Such media could be used for, but not limited to, publicity material, press releases, social media, and website. Consent should also indicate whether agreement has been given to their name being published in any associated publicity. If the subject is less than 18 years of age, then parental/guardian consent should be sought.

Individuals have a right to withdraw consent at any time. If this affects the provision of a service(s) by J&B then the service co-ordinator should discuss with the services manager at the earliest opportunity.

Ensuring the Security of Personal Information

Unlawful disclosure of personal information

1. It is an offence to disclose personal information 'knowingly and recklessly' to third parties.

2. It is a condition of receiving a service that all Customers for whom we hold personal details sign consent before we can provide additional information or marketing not directly associated with providing their service.
3. Individual consent to share information should always be checked before disclosing personal information to another agency.
4. Where such consent does not exist information may only be disclosed if it is in connection with criminal proceedings or in order to prevent substantial risk to the individual concerned. In either case permission of the HR Manager should first be sought.
5. Personal information should only be communicated within J&B 's staff or subcontractors on a strict need to know basis. Care should be taken that conversations containing personal information may not be overheard by people who should not have access to such information.

Ethnic Monitoring

In order for J&B to monitor how well our staff reflect the diversity of the local community we request that they complete an Equality and Diversity Monitoring form. The completion of the form is voluntary, although strongly encouraged. Responses are securely stored and held on a password protected database for statistical purposes.

Use of Files, Books and Paper Records

In order to prevent unauthorised access or accidental loss or damage to personal information, it is important that care is taken to protect personal data. Paper records should be kept in locked cabinets/drawers overnight and care should be taken that personal information is not left unattended and in clear view during the working the day. If your work involves you having personal data at home or in your car, the same care needs to be taken.

Disposal of Scrap Paper, Printing or Photocopying Overruns

Be aware that names/addresses/phone numbers and other information written on scrap paper are also considered to be confidential. Please do not keep or use any scrap paper that contains personal information but ensure that it is shredded.

If you are transferring papers from your home, or from customer's premise, to the office for shredding this should be done as soon as possible and not left in a car for a period of time. When transporting documents, they should be carried out of sight in the boot of your car.

Computers

All our computers are networked therefore access to personal information is restricted by password to authorised personnel only.

Computer monitors that could be viewed via public areas, should be positioned in such a way so that passers-by cannot see what is being displayed. If this is not possible then privacy screens should be used on the monitor to afford this level of protection.

Our server is cloud based therefore integral Firewalls and virus protection is employed at all times to reduce the possibility of hackers accessing our system and thereby obtaining access to confidential records.

Documents should only be stored on the server/ cloud-based systems and not on individual computers.

Where computers or other mobile devices are taken for use off the premises the device must be password protected.

Cloud Computing

When commissioning cloud-based systems, J&B will satisfy themselves as to the compliance of data protection principles and robustness of the cloud based providers.

J&B currently uses cloud based data management systems to hold and manage information about its customers.

Direct Marketing

Direct Marketing communication may be in any of a variety of formats including mail, telemarketing and email. The responses to such should be recorded to inform the next communication to take place. J&B will not share or sell its database(s) with outside organisations.

J&B holds information on our staff, subcontractors, suppliers and customers, to whom we will from time to time send copies of our newsletters, magazine and details of other activities that may be of interest to them. Specific consent to contact will be sought from such before making any communications.

We recognise that clients, staff, volunteers and supporters for whom we hold records have the right to unsubscribe from our mailing lists. This wish will be recorded on their records and will be excluded from future contacts.

The following statement or similar is to be included on any forms used to obtain personal data:

We promise never to share or sell your information to other organisations or businesses and you can opt out of our communications at any time by telephoning 01429 272810, writing to J&B Recycling Ltd, Thomlinson Road, Hartlepool, TS25 1NS, or by accessing the opt out option on our website contact us page at www.jbrecycling.co.uk

Privacy Statements

Any documentation which gathers personal data should contain the following Privacy Statement information:

- Explain who we are
- What we will do with their data
- Who we will share it with
- Consent for marketing notice
- How long we will keep it for
- That their data will be treated securely
- How to opt out
- Where they can find a copy of the full notice

A Privacy Statement will also be published on our website.

Personnel Records

The Regulations apply equally to agency and staff records. J&B may at times record personal data with the volunteer's consent or as part of a staff member's contract of employment.

Confidentiality

When working from home, or from some other off-site location, all data protection and confidentiality principles still apply. All computer data, e.g. documents and programmes related to work for J&B should not be stored on a personal computer or any external hard disk that is not kept permanently in J&B offices. If documents need to be worked on at a non-networked computer, they should be saved onto a USB drive which should be password protected.

Workstations in areas accessible to the public, e.g. reception or weighbridge office, should operate a clear desk practice so that any paperwork, including paper diaries, containing personal and/or special categories of personal data is not left out on the desk where passers-by could see it.

Any paperwork kept away from the office should be treated as confidential and kept securely as if it were held in the office. Documents should not be kept in open view (eg on a desktop) but kept in a file in a drawer or filing cabinet as examples, the optimum being a locked cabinet but safely out of sight is a minimum requirement. Enablers needing to take paperwork away from a client's home (e.g. unable to make a required phone call during the visit) must ensure that it is returned to the client's home on the next visit.

When carrying paper files or documents they should be in a locked briefcase or in a folder or bag, which can be securely closed or zipped up. The briefcase/folder/bag should contain J&B's contact details. Never take more personal data with you than is necessary for the job in hand. Care should be taken to ensure that you leave a customer's premises that you have not inadvertently left something behind.

Retention of Paper Records

Paper records will not be retained for longer than the following periods at the end of which they should be shredded:

- Customer records such as invoices and weighbridge tickets – 7 years after ceasing to be a customer.
- Staff records – 7 years after ceasing to be a member of staff.
- Disciplinary records – 1 month after the expiry date
- Unsuccessful staff application forms – 6 months after vacancy closing date.
- Timesheets and other financial documents – 7 years.
- Employer's liability insurance – 40 years.
- Other documentation such as duty of care documents as per the minimum time specified by other Regulations governing their use

Archived records should clearly display the destruction date.

What to Do If There Is a Breach

If you discover, or suspect, a data protection breach you should report this to your line manager who will review our systems, in conjunction with the Senior Management Team and/or HR Manager, to prevent a reoccurrence. The HR

Manager should be informed of the breach, action taken and outcomes to determine whether it needs to be reported to the Information Commissioner and also to the company Directors. There is a time limit for reporting breaches to ICO so the HR Manager should be informed immediately.

Any deliberate or reckless breach of this Data Protection Policy by an employee or volunteer may result in disciplinary action that may result in dismissal.

The Rights of an Individual

Under the Regulations an individual has the following rights with regard to those who are processing his/her data:

- Data cannot be used for the purposes of direct marketing of any goods or services if the Data Subject has declined their consent to do so.
- Individuals have a right to have their data erased and to prevent processing in specific circumstances:
    - Where data is no longer necessary in relation to the purpose for which it was originally collected
    - When an individual withdraws consent
    - When an individual objects to the processing and there is no overriding legitimate interest for continuing the processing
    - Personal data was unlawfully processed
- An individual has a right to restrict processing – where processing is restricted, J&B is permitted to store the personal data but not further process it. J&B can retain just enough information about the individual to ensure that the restriction is respected in the future.
- An individual has a 'right to be forgotten'.

Data Subjects can ask, in writing to the Managing Director, to see all personal data held on them, including e-mails and computer or paper files. The Data Processor (J&B) must comply with such requests within 30 days of receipt of the written request.

Powers of the Information Commissioner

The following are criminal offences, which could give rise to a fine and/or prison sentence

- The unlawful obtaining of personal data.
- The unlawful selling of personal data.
- The unlawful disclosure of personal data to unauthorised persons.

Further Information

Further information is available at www.informationcommissioner.gov.uk

Details of the Information Commissioner

The Information Commissioner's office is at:

Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Signed: V Jackson-Smith. **Position: Managing Director**

Date: 18th May 2018