Orbic Bearings Limited

Controlled Document

Document Name:	**Data Protection Policy**
Review Schedule	Every two years
Next review due	April 2020
Owner (Responsibility)	Anthony Flint, Director
Pass amendments to:	Tracy Donegan
Revision History	See appendix
Document Location	ISO 9001/2015 Shared Drive

Document Description

This document outlines our legal requirements under the General Data Protection Regulations and the processes for how Orbic Bearings Limited 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 by the Director, 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 accounts@orbic.co.uk or at Orbic Bearings Limited, 187-189 Handcroft Road, Croydon, Surrey, CR0 3LF.
0208 684 8262

Data Protection Policy

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 Orbic Bearings Limited.

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 customers.

All Orbic Bearings Limited staff are required to follow this Data Protection Policy at all times.

The Director has overall responsibility for data protection within Orbic Bearings Limited 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. Orbic Bearings Limited is the Data Controller for the purposes of the Act.
Data Processor – an individual handling or processing data
Personal data – any information which enables a person to be identified
Special categories of personal data – information under the Regulations which requires the individual's explicit consent for it to be held by the Charity.

Data Protection Principles

As data controller, Orbic Bearings Limited 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

Orbic Bearings Limited must record service users' explicit consent to storing certain information (known as 'personal data' or 'special categories of personal data') on file.

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

1. Name and contacts details.
2. Online identifiers such as an IP address & emailed addresses.
3. Payment information, bank details etc.
4. Whether he/she is a member of a trade union.
5. Any modified medical requirements.
6. Any Health & Safety assessments.
7. Any other special categories

As a general rule Orbic Bearings Limited will always seek consent where personal or special categories of personal information is to be held.

It should also be noted that where it is not reasonable to obtain consent at the time data is first recorded and the case remains open, retrospective consent should be sought at the earliest appropriate opportunity.

Obtaining Consent

Consent may be obtained in a number of ways depending on the nature of the records that need to be kept, and consent must be recorded on or maintained with the 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 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 were to be undertaken.

Preliminary verbal consent should be sought at point of initial contact as personal and/or special categories of personal data will need to be recorded either in an email or on a computerised record. The verbal consent is to be recorded in the appropriate fields on the computer record or stated in the email for future reference. Although written consent is the optimum, verbal consent is the minimum requirement.

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.

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. A customer's individual consent to share information should always be checked before disclosing personal information to another agency/supplier.

3. 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 Director should first be sought.

4. Personal information should only be communicated within Orbic Bearings Limited's staff on a strict need to know basis. Care should be taken that conversations containing personal or special categories of personal information may not be overheard by people who should not have access to such information.

Ethnic Monitoring

In order for Orbic Bearings Limited to monitor how well our staff, customers and suppliers reflect the diversity of the local community we may 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 pass worded 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 and special categories of personal information is not left unattended and in clear view during the working the day. If your work involves you having personal / and/or special categories of 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, 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

Where computers are networked, access to personal and special categories of personal information is restricted by password to authorised personnel only.

Computer monitors in the reception area, or other 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. If

working in a public area, e.g. receptions, you should lock your computer when leaving it unattended.

Firewalls and virus protection to be 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 or 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, Orbic Bearings Limited will satisfy themselves as to the compliance of data protection principles and robustness of the cloud based providers.

Direct Marketing

Direct Marketing is a communication that seeks to increase customer base and revenue. The communication may be in any of a variety of formats including mail, telemarketing and email. The responses should be recorded to inform the next communication. Orbic Bearings Limited will not share or sell its database(s) with outside organisations.

Orbic Bearings Limited holds information on our staff, customers and suppliers to whom we will from time to time send copies of any newsletters, magazine and details of other publications that may be of interest to them. Specific consent to contact will be sought from our staff, customers and any suppliers, including which formats they prefer (e.g. mail, email, phone etc) before making any communications.

We recognise that suppliers, staff, and customers 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 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 020 8684 8262 or by writing to Orbic Bearings Limited, 187-189 Handcroft Road, Croydon, Surrey, CR0 3LF or by sending an email to accounts@orbic.co.uk

Privacy Statements

Any documentation which gathers personal and/or special categories of 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 fuller Privacy Statement will also be published on our website.

Personnel Records

The Regulations apply equally to customer and staff records. Orbic Bearings Limited may at times record special categories of personal data with the customer's consent or as part of a staff member's contract of employment.

Confidentiality

Further guidance regarding confidentiality issues can be found in our Confidentiality Policy.

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 Orbic Bearings Limited should not be stored on any external hard disk or on a personal computer. 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 trading 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.

When sending emails to outside organisations, e.g. suppliers, care should be taken to ensure that any identifying data is removed (e.g. initials or email addresses, etc.). Confidential and/or special categories of personal information should be written in a separate document which should be password protected before sending. Wherever possible, this document should be 'watermarked' confidential.

Any paperwork kept away from the office (e.g. personal data kept at home by a worker) should be treated as confidential and kept securely as if it were held in the office. Documents should not be kept in open view (e.g. 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.

Retention of Records

Paper records should be retained for the following periods at the end of which they should be shredded:

- Supplier records – 6 years after ceasing to be a supplier.
- Staff records – 6 years after ceasing to be a member of staff.
- Unsuccessful staff application forms – 6 months after vacancy closing date.
- Volunteer records – 6 years after ceasing to be a volunteer.
- Timesheets and other financial documents – 7 years.
- Employer's liability insurance – 40 years.
- Other documentation should be destroyed as soon as it is no longer needed for the task in hand.

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 the systems, in conjunction with the Data Compliance Officer, to

prevent a reoccurrence. The Director should be informed of the breach, action taken and outcomes to determine whether it needs to be reported to the Information Commissioner and for reporting to Orbic Bearings Members. There is a time limit for reporting breaches to ICO so the Director should be informed without delay.

Any deliberate or reckless breach of this Data Protection Policy by an employee may result in disciplinary action which 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:

- Personal and special categories of personal data cannot be held without the individual's consent.

- 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, Orbic Bearings Limited is permitted to store the personal data but not further process it. Orbic Bearings Limited 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'.

Orbic Bearings Limited will not undertake direct telephone marketing activities under any circumstances.

Data Subjects can ask, in writing to the Non-Executive Chairman, to see all personal data held on them, including e-mails and computer or paper files. The Data Processor (Orbic

Bearings Limited) 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

Switchboard: 01625 545 700
Email: mail@ico.gsi.gov.uk
Data Protection Help Line: 01625 545 745
Notification Line: 01625 545 740

Revision History

Revision date	Summary of Changes	Other Comments
8th April 2020	Routine review of any updates to GDPR Policy	