Privacy Policy

Table of Contents

Table of Contents....2
Introduction....3
Definitions....3
Data Controller....3
Data Subject....3
Personal Information....3
Sensitive information....3
Data Processing....3
Legislation....3
Governance....4
Roles and Responsibility....4
Board Level....4
Data Protection Officer....4
Staff Responsibilities....4
Reporting....4
Risk Management....4
Data Privacy Impact Assessment (DPIA)....4
Risk Register....4
Privacy Principles....4
Collecting Information....4
Processing Information....4
Securing Information....5
Deleting data retention....5
Subject Access Request and Data Transfer Request....5
Communication....5
Education and Awareness....6
Incident Handling....6
Assurance and compliance....6
Annex A - Retention Schedule....7

Introduction

Porvair Filtration Group Ltd needs to collect and use information on individuals such as customers, potential customers, suppliers and staff members. We use this information to manage our business, meet our contractual obligations with the customer and meet our legislative requirements. However, we must ensure that we use and protect the information in accordance with current legislation. Failure to do so could lead to distress to individuals, financial sanctions from the Information Commissioners Office (ICO), reputational damage and impair our ability to attract new customers.

This policy, together with Porvair's Access Control Policy, describes how we will safeguard personal information to protect the individual and comply with the law.

Privacy Policy

Definitions

Data Controller
Porvair Filtration Group Ltd is the data controller for the personal information we collect such as our employee information and business contact information. We are registered with the ICO, and we are responsible for protecting this information in accordance with this policy.

Data Subject
The data subjects are the individuals whose personal information we deal with such as customers, potential customers, suppliers and staff members.

Personal Information
Personal information means any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, from the information. The information includes name, address, date of birth, email, telephone number, national insurance number etc. Personal information also includes information associated with that individual such as telephone bills, call recordings, staff development, staff reviews and pay rates. Personal information also includes opinions on an individual and any intention that we may have towards that individual. We must therefore be cautious what we record on personnel files.

Sensitive information
Sensitive information, such as medical, race, religion, sexuality, political or trade union membership, is a special category of data that requires sensitive handling.

Data Processing
Processing means any action performed on personal information, which includes collection, recording, organising, storing, sharing and transmitting. This includes electronic and paper documents containing personal information. Many of the activities within Porvair Filtration Group Ltd involves processing information and therefore we must comply with the law.

Legislation
Porvair Filtration Group Ltd must comply with the Data Protection Act (DPA) 2018 and the EU General Data Protection Regulation (GDPR).

Governance

Roles and Responsibility
Everyone associated with Porvair Filtration Group Ltd has a responsibility to ensure we protect the personal information we hold and comply with this policy.

Board Level
The HR Manager is accountable for data privacy and will report to the board on data privacy every quarter.

Data Protection Officer
The HR Manager has day-to-day responsibility for data privacy, and is the main point of contact for any questions about data privacy.

Staff Responsibilities
All staff are responsible for complying with this policy.

Reporting
The HR Manager will produce an annual report on data privacy for the board of directors.

Privacy Policy

Risk Management

Data Privacy Impact Assessment (DPIA)
When we are considering processing information in a new way, using a new technology or processing sensitive information, the HR Manager will decide whether a Data Privacy Impact Assessment (DPIA) is required.

Risk Register
The HR Manager will maintain the Porvair's Filtration Group's Privacy Risk Register. The register will be reviewed annually by the board of directors.

Privacy Principles

Collecting Information
We should collect the minimum personal information we need to complete a task. We should not collect information just in case. If someone is making an enquiry about our services we should only collect initial contact details, there is no need to collect further information as these can be added later.

Processing Information
When we are planning to process information, we need to consider the legal reason for processing, and whether we need the individual's consent to process. Much of our processing is for legitimate business reasons to run our business and deliver our contracted services to customers; we need to pay staff, monitor and report on services and invoice fees and therefore we do not require consent.

However, some activities may not be considered necessary to deliver the contracted services, such as marketing. Where we are marketing to business customers we do this as a legitimate business interest and do not need their consent, but we must offer them the right to opt-out of further communications. Where a business customer opts-out we must record this and ensure we do not market to that customer again.

We must not send marketing material to an individual's personal email address or home address without their consent.

In the event that the business choose to use data for unsolicited communication the Marketing Manager will maintain a Processing Register.

Securing Information

We must protect the personal information we use whether in electronic or paper format.

- Documents containing personal information should be stored securely when not required.
- Documents containing staff personal information should only be removed from business premises where necessary. Documents must be protected while off site and should not be left unattended.
- Electronic copies of personal information must be stored on Porvair Filtration Group Ltd controlled devices or systems in accordance the PFG IT policy.

Deleting data retention
When personal information is no longer required, and there is no legal requirement to retain the information, electronic data must be deleted, and paper copies securely destroyed. Annex A contains a list of how long we need to retain the types of information we process.

Subject Access Request and Data Transfer Request

Individuals have the right to know whether we store and process their personal information, this is known as a Subject Access Request. If the information we hold is inaccurate they have the right for that information to be corrected. In certain circumstances, they have the right to have the information deleted or to be given a copy of that information. We have to respond to any request within 30 days. The individual does not have to state they are making a subject access request, it can be a simple email asking what information we hold, and therefore, any request by an individual with regards to the information we hold must be forwarded to the HR Manager.

Communication

Privacy Policy

Porvair Filtration Group Ltd is registered with the ICO as a data controller and data processor. The HR Manager is responsible for maintaining our registration.

We will have a privacy notice which will clearly inform individuals how we collect their information, what we do with their information and their rights. A copy of the privacy notice will be displayed prominently on our website and a copy will be sent to individuals when we are requesting information from them.

Where we are delivering a service as a data processor the relevant privacy notices will be included in the terms and conditions of the contract.

The privacy notice for staff will be given to staff on induction.

The HR Manager is responsible for maintaining the privacy notice.

Email Marketing

Whilst you use our website we may collect information that is personally identifiable as part of our legitimate interest, such as contact details. Information that you provide on a contact form, to allow us to respond to your enquiry or to provide you with the information / communications that you have requested.

Education and Awareness

All new joiners including temporary staff must read this data privacy policy as part of their induction process.

All staff will receive data privacy policy as part of their ongoing staff development. The HR Manager will periodically send emails to all staff highlighting key aspects of data privacy.

Incident Handling

We have a legal responsibility to report certain data privacy incidents to the ICO within 72 hours or face a financial penalty. It is essential all staff follow the incident procedure. Example of privacy breaches are:

- Revealing a customer's contact details to an unauthorised third party.
- Accidentally emailing an employee's sensitive personal information to an unauthorised member of staff or third party.
- Losing a laptop containing the personal information of a large number of customers and staff.

Not all the examples above are reportable to the ICO however it is essential that staff report any incident or potential incident to the HR Manager. The HR Manager will then discuss the incident with the board of directors and decide whether the incident requires reporting to the ICO and whether an action is required to manage the risks from the incident.

Assurance and Compliance

The HR Manager & IT Manager will carry out periodic review of processes and update the policy as necessary.

Annex A - Retention Schedule

The primary actors that inform decisions on retention are:

- Business need – as agreed by the organisation and their HR policy.
- Legislative and regulatory requirements.
- National Archives requirements and guidelines.

It is important that the retention schedule is kept up-to-date, to reflect changing business needs, new legislation, changing perceptions of risk management and new priorities for the organisation.

It should be noted that personal data should not be kept longer than is necessary for the purpose or purposes for which it is being processed. So, this means you'll need to apply some judgment and apply different holding times for different types of personal data. It is essential you ensure that manual records be shredded and electronic files permanently deleted from the system.

Privacy Policy

Example of retention schedule:

Type of Record	Retention Period
Customer	
Financial transaction records	6 years after end of financial year
Contracts	6 years after account is closed
Letters	6 years after account is closed
Complaints	6 years after account is closed
Enquiries	3 years after account is closed
Investigations	10 years after account is closed
Staff	
Job application and interview records	6 months following unsuccessful application
Personnel records	7 years after employment ceases
Training records/appraisals	7 years after employment ceases
Employment agreements	7 years after employment ceases
Payroll and wage records (including details of overtime, bonuses and expenses)	7 years after employment ceases
Salary records	7 years
Disciplinary warnings should be removed from employee's personnel files once they have expired	Oral warning – 6 months Written warning – 12 months Final warning – 18 months
Disciplinary action ever taken, in particular disciplinary hearings	7 years after employment ceases
Grievance issues	7 years after employment ceases
Termination: The process of termination of staff through voluntary redundancy, dismissal and retirement	7 years after employment ceases
Details of benefits in kind	7 years after employment ceases
Financial	
Income tax records (P45/P60/P11d's etc.)	7 years
Annual return of taxable pay and tax paid	7 years
Published accounts	12 years
Tax returns	12 years
Financial records held on general ledgers	12 years
Health & Safety	
Accident/Incident Book	15 years
Legal/Accident/Incident Forms	4 years from date of accident
Risk Assessments	7 years
Health & Safety Reports	15 years
Fire Procedure	Until superseded but retain copies of earlier versions

Type of Record	Retention Period
Health & Safety Policy	Until superseded but retain earlier versions up to 15 years and review as necessary
Records of monitoring areas where employees are likely to come into contact with asbestos.	Retain for 40 years (refer to The Control of Substances Hazardous to Health Regulations 2002)
Fire log books	Retain for 7 years
Legal	
Third party contracts	6 years after date of termination (unless signed as a deed, in which case 12 years after date of termination)
Other	
Policies	6 years from the date they cease to be relevant
Procedures	6 years from the date they cease to be relevant
Company Secretarial Records (eg board meeting minutes)	Permanently
CCTV	30 days