DATA PROTECTION POLICY

Contents

1. **Introduction** 2
2. **Data Protection Principles** 2
3. **Data protection by design & by default** 3
4. **Data Security** 4
5. **Training** 5
6. **Other Policies** 5
7. **Forms** 5

SCHEDULE 1: DOCUMENT RETENTION 5

SCHEDULE 2: SUBJECT ACCESS REQUESTS (SAR) 10

SCHEDULE 3: DATA PROTECTION IMPACT ASSESSMENT (DPIA) 11

SCHEDULE 4: PERSONAL DATA BREACH RESPONSE 11

REVISION HISTORY				
Rev.	**Effective Date**	**Description**	**Code**	**Owner**
00	January 2023	Newly Implemented	DP-PO-EH-NS-001	HR
01	December 2023	Reviewed since MBO	HR-PO-GP-023	Stacey Walker – Head of HR
02	June 2024	Updated document retention	HR-PO-GP-023	Stacey Walker – Head of HR
03	September 2024	Removal of third party DPO	HR-PO-GP-023	Stacey Walker – Head of HR

**This document is 'Uncontrolled' when printed. Please refer to the share point for the latest version*

DATA PROTECTION POLICY

1. Introduction

This policy sets out the company's commitment to data protection, and individual rights and obligations in relation to personal data.

This Data Protection Policy is the overarching policy for data security and protection for HSP Valves Group (hereafter referred to as "us", "we", or "our").

The purpose of the Data Protection Policy is to support the 10 Data Security Standards, the UKGDPR, the Data Protection Act (2018), the common law duty of confidentiality and all other relevant national legislation. We recognise data protection as a fundamental right and embrace the principles of data protection by design and by default.

This policy covers our data protection principles and commitment to common law and legislative compliance and our procedures for data protection by design and by default.

This policy applies to all staff, including temporary staff and contractors.

This policy includes in its scope all data which we process either in hardcopy or digital copy, this includes special categories of data.

For all immediate needs relating to Data protection and this policy, please email the data protection team on dataprotection@hsp-valves.com. The data protection team is made up of the Managing Director and HR.

2. Data Protection Principles

3.1 We will be open and transparent with service users and those who lawfully act on their behalf in relation to their care and treatment.

3.2 We will establish and maintain policies to ensure compliance with the Data Protection Act 2018, Human Rights Act 1998, the common law duty of confidentiality, the General Data Protection Regulation and all other relevant legislation.

3.3 We will establish and maintain policies for the controlled and appropriate sharing of service user and staff information with other agencies, taking account all relevant legislation and citizen consent.

3.4 Where consent is required for the processing of personal data we will ensure that informed and explicit consent will be obtained and documented in clear, accessible language and in an appropriate format. The individual can withdraw consent at any time through processes which

have been explained to them and which are outlined in our Record Keeping Policy: Withdrawal of consent procedures. We ensure that it is as easy to withdraw as to give consent.

3.5 We will commission annual audits of our compliance with legal requirements.

3.6 We acknowledge our accountability in ensuring that personal data shall be:

- Processed lawfully, fairly and in a transparent manner;
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
- Accurate and kept up to date;
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed ('storage limitation');
- Processed in a manner that ensures appropriate security of the personal data.

3.7 We uphold the personal data rights outlined in the GDPR;

- The right to be informed;
- The right of access;
- The right to rectification;
- The right to erasure;
- The right to restrict processing;
- The right to data portability;
- The right to object;
- Rights in relation to automated decision making and profiling

3. Data protection by design & by default

4.1 We shall implement appropriate organisational and technical measures to uphold the principles outlined above. We will integrate necessary safeguards to any data processing to meet regulatory requirements and to protect individual's data rights. This implementation will consider the nature, scope, purpose and context of any processing and the risks to the rights and freedoms of individuals caused by the processing.

4.2 We shall uphold the principles of data protection by design and by default from the beginning of any data processing and during the planning and implementation of any new data process.

4.3 Any new high-risk data processing activities will be assessed using a Data Privacy Impact Assessment (DPIA) before the processing commences – See Schedule 3.

4.4 All new systems used for data processing will have data protection built in from the beginning of the system change.

4.5 All existing data processing has been recorded on our Record of Processing Activities. This is reviewed annually.

4.6 We ensure that, by default, personal data is only processed when necessary for specific purposes and that individuals are therefore protected against privacy risks.

4.7 In all processing of personal data, we use the least amount of identifiable data necessary to complete the work it is required for and we only keep the information for as long as it is required for the purposes of processing or any other legal requirement to retain it.

4. Data Security

The company has internal policies and controls in place to protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties. For further details on this please refer to the linked policies in under section 7.

Where the company engages third parties to process personal data on its behalf, such parties do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

5.1 International Data Transfers

The company will not transfer personal data to countries outside the UK.

5.2 Individual Responsibilities

Individuals are responsible for helping the company keep their personal data up to date. Individuals should let the company know if data provided to the company changes, for example if an individual moves house or changes bank details.

Individuals may have access to the personal data of other individuals and of our customers and clients in the course of their employment, contract, volunteer period, internship or apprenticeship. Where this is the case, the company relies on individuals to help meet its data protection obligations to staff and to customers and clients.

Individuals who have access to personal data are required:

- to access only data that they have authority to access and only for authorised purposes;
- not to disclose data except to individuals (whether inside or outside the organisation) who have appropriate authorisation;
- to keep data secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction);
- not to remove personal data, or devices containing or that can be used to access personal data, from the organisation's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device;
- not to store personal data on local drives or on personal devices that are used for work purposes; and
- to report data breaches of which they become aware to dataprotection@hsp-valves.com immediately.

Further details about the organisation's security procedures can be found in its IT security policy and other linked policies detailed in section 7.

Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under the company's disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing employee or customer data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

5. Training

The company will provide training to all individuals about their data protection responsibilities as part of the induction process and as part of our annual compliance training process.

6. Other Policies

Employees are encouraged to read this policy in conjunction with other relevant Company policies, including but not limited to:

- IT Security Policy
- Acceptable Use Policy
- Employee Privacy Notice

7. Forms

- Subject Access Request Form (SAR)
- Data Protection Impact Assessment (DPIA) Form

SCHEDULE 1: DOCUMENT RETENTION

Facilities

TYPES OF RECORDS	PERIOD	STARTING FROM
Donation record	3 years	End of relevant financial year
Office premises and company house purchase/ lease / sale alteration record	7 years	From completion of disposal
Documents of office insurance	3 years	Expiry date
Equipment/Plant maintenance records (inc. PAT)	5 years	Date the equipment is no longer in use
Calibration Records - Measuring/ Test Equipment	5 years	Date the equipment is no longer in use

Business Planning

TYPES OF RECORDS	PERIOD	STARTING FROM
Organisation documents	10 years	End of relevant financial year
Budget and business planning	3 years	End of relevant financial year
Monthly report	1 year	End of relevant financial year
Conference minutes	3 years	Date of conference
Company minute books	Permanent	
Company registers	Permanent	
Articles of association, memorandum of incorporation	Permanent/3 years	Permanent/Disposal date
Shareholders agreement or other investment agreement (not executed as deeds)	6 years	The earlier of the expiry, termination or disposal date
Shareholders agreement or other investment agreement executed as deeds	12 years	The earlier of the expiry, termination or disposal date
Documents relevant to legal proceedings including internal application and approval–contracts (not signed as a deed)	6 years	Expiry or earlier termination date of any relevant agreement unless there is a "litigation hold"
Documents relevant to legal proceedings including internal application and approval– deed	12 years	Expiry or earlier termination date of any relevant agreement unless there is a "litigation hold"
All company used system data (ie Soft, CRM, Project Based)	5 years	Following end of relevant job expiry

Commercial Projects

TYPES OF RECORDS	PERIOD	STARTING FROM
Quotation Files	1 year (where order is lost)	Date of last quotation
Job Files (excluding documentation dossiers – see CON0200)	7 years unless stipulated longer under the requirements of the contract	Date of close out of relevant job

All documents required to be preserved by a regulatory authority	For period stipulated by regulatory authority	From date stipulated by regulatory authority
Stock Orders	Determined by contract	-
Design Related Records	Indefinitely	-

QHSE

TYPES OF RECORDS	PERIOD	STARTING FROM
Non-conforming/correction action records, such as defect notes, corrective action requests etc.	5 years	From the date of closure
QHSE Audits/Inspections	5 years	From the date of Audit/Inspection Completion
Risk Assessments (inc. DSE & Manual Handling)	5 years	After the assessment has ceased to be relevant, e.g.: any required changes have been made or met
COSHH Assessments (inc related SDS)	5 years	After the product is no longer in use
PPE and issuance of PPE records	Indefinitely	-
Records associated with Fire Equipment	5 years	After the equipment is no longer in use
Fire Safety and Inspection Records	Indefinitely	-
RIDDOR/Accident records	6 years	After the incident date
Waste Transfer Notes	2 years	After the note
Special/Hazardous Waste Consignment Notes	3 years	After the note
Waste Carrier Certificate of Registration	5 years	From the date of expiry
QHSE Health Surveillance Records (Hazardous substances such as COSHH)	40 years	From the date of last entry
All other QHSE system related records	7 years	Date of leaving
Supplier Assessments	5 years	From end of relationship

Human Resources

TYPES OF RECORDS	PERIOD	STARTING FROM
Individual personal file (including CV, contract, copy of identification, sickness records, visa documents)	7 years	Date of leaving
Payroll Files or related document	7 Years	End of relevant financial year
Pension documents	12 years	After benefit ceases
Rejected job application records, including; application letters/forms, CVs, references, certificates of good conduct, interview notes etc	1 year	After applicant is notified of rejection
Disciplinary Record	As determined during process	From the date of sanction
Personal Data		
Training Records	7 years	Date of leaving
Personal Detail Records (Bank Details, Emergency contact, Next of Kin, Contact details)	3 months	Leave date or following final payment being made within payroll

Finance

TYPES OF RECORDS	PERIOD	STARTING FROM
Company credit card (statement)/(application)	1 year	End of relevant financial year
Company credit card (cancellation)	1 year	Date of cancellation
Accounting rules and internal procedures	Permanent	
VAT return and supporting evidence	7 years	End of relevant financial year
Corporation tax return and supporting evidence (including withholding tax certificates)	7 years	End of relevant financial year
Balance sheet and profit & loss statement for the financial year	7 years	End of relevant financial year

(Signed) audited financial statements (including working schedules)	Permanent	
Sales invoices	7 years	End of relevant financial year
Disbursement slip and supporting evidence	7 years	End of relevant financial year
Bank reconciliations	7 years	End of relevant financial year
Bank statements	7 years	End of relevant financial year
Inventory: monthly warehouse	7 years	End of relevant financial year
Inventory: annual stock check report and supporting schedules	7 years	End of relevant financial year
Inventory impairment schedules	7 year	End of relevant financial year
Fixed asset and depreciation details	7 years	End of relevant financial year after the asset is written off or disposed
Balance confirmation reports: accounts receivable, loans receivable etc.	5 years	End of relevant financial year
Monthly report and analysis on financial results	5 years	End of relevant financial year
Budget analysis and reports	5 years	End of relevant financial year
Management approval for bank transaction	Permanent	
Bank authority and signature card	7 years	Date of cancellation
Bank charges	3 years	End of relevant financial year
Bank interest	3 years	End of relevant financial year
Bank statements (accts)	7 years	End of relevant financial year
Bank reconciliation records	7 years	End of relevant financial year
Application for loan/application for deposit	3 years	End of relevant financial year
Copies of opened/received letters of credit	3 years	End of relevant financial year

Copies of opened/received letters of guarantee	3 years	End of relevant financial year
Used foreign exchange contracts	7 years	End of relevant financial year
Credit report	1 year	Expiry date of validity
Customs Documents	Permanent	

SCHEDULE 2: SUBJECT ACCESS REQUESTS (SAR)

Individuals have the right to make a subject access request. If an individual makes a subject access request, the company will tell them:

- whether their data is processed and if so why, the categories of personal data concerned and the source of the data if it is not collected from the individual;
- to whom their data is or may be disclosed, including to recipients located outside the UK and the safeguards that apply to such transfers;
- for how long their personal data is stored (or how that period is decided);
- their rights to rectification or erasure of data, or to restrict or object to processing;
- their right to complain to the Information Commissioner if they think the organisation has failed to comply with their data protection rights; and
- whether the company carries out automated decision-making and the logic involved in any such decision-making.

The company will also provide the individual with a copy of the personal data undergoing processing. This will normally be in electronic form if the individual has made a request electronically unless they agree otherwise.

An individual can make a SAR verbally or in writing, including on social media. A request is valid if the individual is asking for their own personal data. An individual does not need to use a specific form of words, refer to legislation or direct the request to a specific contact.

An individual may ask a third party (e.g. a relative, friend or solicitor) to make a SAR on their behalf.

Before responding, the company will need to be satisfied that the third party making the request is entitled to act on behalf of the individual. It is the third party's responsibility to provide evidence of their authority.

If the individual wants additional copies, the company will charge a fee, which will be based on the administrative cost to the organisation of providing the additional copies.

To make a subject access request, the individual should send the request to dataprotection@hsp-valves.com or use the company's form for making a subject access request. In some cases, the

company may need to ask for proof of identification before the request can be processed. The company will inform the individual if it needs to verify their identity and the documents it requires.

The company will normally respond to a request within a period of one month from the date it is received. In some cases, such as where the request is complex, it may respond within three months of the date the request is received. The company will write to the individual within one month of receiving the original request to tell them if this is the case.

If a subject access request is manifestly unfounded or excessive, the company is not obliged to comply with it. Alternatively, the company can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request. A subject access request is likely to be manifestly unfounded if it is made with the intention of harassing the company or causing disruption,

or excessive where it repeats a request to which the company has already responded. If an individual submits a request that is unfounded or excessive, the company will notify them that this is the case and whether it will respond to it.

SCHEDULE 3: DATA PROTECTION IMPACT ASSESSMENT (DPIA)

A Data Protection Impact Assessment (DPIA) should be carried out where the business is looking to complete any new high-risk data processing activities that will involve the processing of personal data and is likely to result in a high risk to the rights and freedoms of individuals.

A DPIA must be conducted at the start of any new project involving processing of personal data, or as soon at it becomes evident that a high-risk process is being carried out.
High Risk Operations may include but are not limited to:

- Extensive automated decision making with significant affect to individuals
- Large scale processing of special categories of personal data
- Large scale processing of personal data relating to criminal convictions
- Systematic monitoring of publicly accessible areas on a large scale
- The introduction of new technology / systems used to process personal data
- The combination or comparison of data from multiple sources
- Processing personal data where the individual is not directly informed
- Processing the personal data of children, especially for marketing purposes
- Where a personal data breach could result in physical harm to individuals

Where a DPIA indicates that a high-risk operations cannot be mitigated against by the introduction of reasonable safeguards or security measures, the company should contact the data protection team dataprotection@hsp-valves.com who will contact our Data Protection Officer for support.

All complete DPIA should be sent to the data protection team for final review and should be stored along with the project it was intended for as proof of completion.

SCHEDULE 4: PERSONAL DATA BREACH RESPONSE

The Data Protection legislation typically requires Data Controllers to report any data breaches to the relevant supervisory authority where the breach is likely to result in a high risk of adversely affecting Individuals' rights and freedoms, the Company must also inform those Individuals without undue delay.

The Company will maintain a record of all Personal Data breaches, regardless of their severity on the data protection register.

What is a Personal 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. This includes breaches that are the result of both accidental and deliberate causes. It also means that breach is more than just about losing Personal Data.

Reporting a Breach

Where an employee becomes aware of a Personal Data Breach or potential breach, they must notify the Data Protection Team (dataprotection@hsp-valves.com) immediately as the Company has strict obligations to report breaches quickly. A delay could put the Company in breach of its obligation under the data protection legislation and at risk of investigation or enforcement action, including large fines. Failure to report a personal data breach may result in disciplinary action being taken.

As soon as practical after the report of a Personal Data Breach we will look to arrange a meeting with the reporter of the Personal Data Breach, and any other persons that may assist in dealing with the Personal Data Breach.

When a breach is reported the Company will endeavour to:

- Identify the cause of the Personal Data Breach
- Establish what steps can or need to be taken to contain the breach from further data loss
- Undertake an investigation immediately and wherever possible within 24 hours of the breach being discovered / reported and assess the risks associated with it
- Contact all relevant persons who are or may be able to assist in the process
- Determine what can be done to recover loss – e.g. recovery of data use of back-up data
- Where appropriate, shall consider informing the police/banks
- Log all actions taken to contain the issue

The investigation of a data breach will take into account the following:

- The type of data involved
- Its sensitivity
- The protections that are in place, for example encryptions
- What has happened to the data, for example if it has been lost or stolen
- Whether the data could be put to any illegal or inappropriate use
- Data subject(s) affected by the breach, number of individuals involved and the potential effects on those data subject(s)
- Whether there are wider consequences to the breach

The Company will establish whether it is necessary to notify the data protection authorities in the relevant jurisdiction and if so, where feasible ensure that they notify them within the required timeframe. For example, in the UK, this would be the Information Commissioner's Office (ICO) and the notification timeframe, where feasible, is within 72 hours of becoming aware of the breach.

Every data breach will be assessed on a case-by-case basis

Individuals whose personal data has been affected by the data breach, and where it has been considered likely to result in a high risk of adversely affecting that individual's rights and freedoms, will be informed without undue delay.

The company may consider notifying third parties such as the police, insurers, banks or credit card companies, and trade unions. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future.

Evaluation & Response

Once the data breach is contained, the company will carry out a full review of the causes of the breach, the effectiveness of the response(s) and whether any changes to systems, policies and procedures should be undertaken.