PSPS

Public Sector Partnership Services Ltd

Data Protection Policy

20/05/2024

1. Document Control

Version Control

Issue	Author	Date	Reason for Issue
0.1	M Elsom	Jan 2018	Initial draft for review
0.2	M Elsom	May 2018	Revised in readiness for 25 May and to align with Information Governance Framework approach
2.0	M Elsom	October 2018	Amended to included direct reference to DPIA
3.0	M Elsom	October 2020	Amended to reference special category processing and DPO role appointment
4.0	M Elsom	July 2022	
4.1	M Elsom	August 2022	Small amendment to Section 7 to reference agile/home working and associated policy
5.1	M Elsom	May 2024	Review – minor amends, plus inclusion of AI

Approval Control

Issue	Approval Authority	Name	Approval	Due for Review
1.0	Head of Operations	Lewis Ducket	25/05/2018	25/05/2020
2.0	Head of Operations	Lewis Ducket	31/10/2018	31/10/2020
3.0	Board of Directors	Chair of the Board	19/10/2020	31/10/2022
4.0	Board of Directors	Angela Newton, Chair	25/07/2022	31/07/24
5.0	Chief Executive	Lewis Ducket	01/09/2022	30/09/2025
6.0	Board of Directors	Jim Astill, Chair	20/05/2024	20/05/2027

Policy Governance

Responsible	PSPS Chief Executive (Senior Information Risk Owner or 'SIRO') and Head of Corporate Services (Data Protection Officer or 'DPO')
Accountable	PSPS Board of Directors
Consulted	PSPS – Chief Delivery Officer
Informed	PSPS Employees

2. Policy Overview

To define the framework and roles through which Public Sector Partnership Services Limited (also referred to in this policy as PSPS or 'the company') will demonstrate accountability and compliance with regards to data protection law.

3. Introduction

3.1. The UK General Data Protection Regulation (GDPR) and the Data Protection Act (2018) regulate the processing of personal data.

3.2. The Privacy and Electronic Communications Regulations sit alongside Data Protection Law and give people specific privacy rights in relation to electronic communications.

3.3. The Information Commissioner's Office (ICO) is the regulator responsible for upholding information rights in the public interest.

3.4. This policy defines the company's approach to being legally compliant through provisions promoting accountability and governance.

4. Our Commitment

4.1. All personal data will only be processed in accordance with data protection law.

4.2. PSPS will appoint a Data Protection Officer (DPO) who will be responsible for ensuring that appropriate data protection governance arrangements and controls are in place.

4.3. PSPS will create and maintain records management processes for all electronic and manual records containing personal data. This should include consideration of timely and secure destruction, as well as data categorisation to reduce the risk of data leakage.

4.4. The Company will have a consistent approach for dealing with Data Subject Rights requests, to facilitate consistent and lawful practice. This will include dealing with Subject Access Requests (SARs).

4.5. PSPS will ensure that technical and organisational measures are in place to ensure there is adequate security over personal data held in manual or electronic form.

4.6. The Company will ensure that all employees receive sufficient data protection training and associated information relating to their roles and responsibilities.

4.7. PSPS will design and operate suitable procedures and controls to allow for the sharing of information only in ways that comply with data protection law.

4.8. The Company will implement measures that meet the principles of data protection by design and data protection by default, such as data minimisation, pseudonymisation, transparency, monitoring and improved security features. In support of this approach, Data Protection Impact Assessments (DPIAs) will be completed as standard for any significant project, task or other change activity that requires the processing of personal data.

4.9. PSPS will engage and work collaboratively with its client councils and process according to their instructions where they act as data controller. The councils will be granted oversight of all information management related processes upon request.

5. Data Protection Principles

5.1. PSPS will ensure that all data processing is carried out according to the data protection principles as defined in Article 5 of the UK GDPR, which states that personal data shall be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals.
- 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.
- Accurate and, where necessary, 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 is processed.
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

6. Special Category Personal Data

6.1. PSPS is required to process special category personal data, which needs more protection because it is sensitive.

6.2. Where the company processes special category personal data it will do so lawfully by identifying a lawful basis under Article 6 of the GDPR and a separate condition for processing under Article 9.

6.3. Information Asset Registers will serve as our record of processing activity (ROPA) and will define the condition relied upon, how the processing satisfies Article 6 of the GDPR (lawfulness of processing), and whether the personal data is retained and erased in accordance with the retention policies.

6.4. Where required, an appropriate policy document will be in place to meet a UK Schedule 1 condition for processing in the DPA 2018.

7. Using Third Party Processors

7.1. The company acknowledges that using third-party service providers is necessary for service delivery, where processing arrangements will require the sharing of personal data with the supplier.

7.2. PSPS will ensure that, in such circumstances, appropriate contracts and/or Information Sharing Agreements are in place.

8. Breaches and Offences

8.1. The DPO is responsible for ensuring that an effective Breach Management Procedure is in operation, which should ensure that all personal data breaches and near misses are managed in such a way as to reduce the risk to data subjects and the company. Immediate remedial action should be taken to reduce the risk, and an investigation should be completed to establish lessons learned and to ensure changes are made to reduce the risk of reoccurrence.

8.2. PSPS will inform its client councils as soon as possible where they are the data controller, and within 24 hours wherever possible. Full oversight will be provided to the relevant council(s) throughout the process of remediation, investigation, and implementation of mitigations against reoccurrence. In such breaches, the council will decide whether to report the breach to the ICO, and PSPS will endeavor to support them as required.

8.3. In the event of a data breach where PSPS is the data controller, and where there is a high risk of adversely affecting an individuals' rights and freedoms, PSPS will report the data breach to the ICO within 72 hours of becoming aware.

8.4. Any deliberate breach of the rules and procedures identified in this policy and associated framework documentation will likely constitute an offence according to the law and could result in disciplinary action.

8.5. PSPS will ensure that adequate insurance is in place to protect against the possible financial implications of data breach and/or cyber-attacks.

9. Artificial Intelligence

9.1. PSPS is open to opportunities for using artificial intelligence (AI) to improve its services and develop efficiency savings, but there are risks inherent to AI and the Company is committed to implementing AI cautiously, intelligently, and with due care and consideration to privacy and other related data protection risks.

9.2. Any PSPS employee involved in implementing and/or managing AI solutions should do so in accordance with the Artificial Intelligence Policy, which sets out to ensure the use of AI is ethical, lawful, and in accordance with all other policies. In relation to data protection, the Artificial Intelligence Policy sets out that approval is required from the DPO before using AI, and that a DPIA should be completed in full to ensure all ethical and technical risks are considered and managed appropriately.

10. Roles and Responsibilities

10.1. The following roles are those formally defined within the Policy:

Role	Responsibility
Senior Information Risk Owner (SIRO)	A role undertaken by the Chief Executive Officer, who retains overall accountability for information risks across the organisation.
Data Protection Officer (DPO)	A role undertaken by the Head of Corporate Services, who is responsible for: Informing and advising the organisation and its employees about their obligations to comply with data protection law. Monitoring compliance to data protection law, including managing internal data protection activities, advising on data protection impact assessments, training employees, and conducting (or commissioning) internal audits. Being the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc.).
Deputy DPO	A role undertaken by the Chief Delivery Officer, who is responsible for: Acting as DPO in the event of DPO absence or any conflict of interest relating to the DPO's remit. Ensuring that organisational technical measures are in place and adequate for the protection of personal data being processed.
Information Asset Owners (IAO)	IAOs are responsible for the day-to-day operation and associated processing of personal data specific to their job roles. They should be able to advise on suitable retention periods, will manage the Information Asset Registers, and oversee compliance within their service.

10.2. PSPS is committed to ensuring the occupants of the above roles act with complete objectivity where there is no conflict of interest. To help achieve this:

- PSPS will ensure that the DPO occupies a position of enough seniority to influence organisational decision-making, but with no or very minimal direct operational responsibility for the processing of personal data.
- If a conflict of interest exists, such as decisions affecting operational matters within the DPO's direct remit, the deputy DPO should assume DPO responsibilities.
- The assigning of the above roles should be scrutinised and reviewed as part of each Policy review and subsequent approval.

10.3. Other key responsibilities can also be broadly defined as follows:

- **Heads of Department** retain overall accountability for Information Assets processed within their department, and for ensuring that suitably skilled and experienced officers are assigned as Information Asset Owners.
- All **PSPS Team Members** have a responsibility for completing training opportunities provided and for complying according to all related internal Policies and Procedures.
- All **PSPS Employees** have a responsibility for ensuring they work in accordance with and uphold all data protection principles regardless of their location of work. This includes a responsibility for ensuring home working arrangements are suitable, safe and secure, in accordance with the Data Protection Policy, the PSPS Agile Working Policy, and the ICT Acceptable Usage Policy. No third party should have unauthorised access to any data controlled by either PSPS or its client Councils.
- The person responsible for procuring and contracting services from a third-party service provider is responsible for ensuring that adequate contract arrangements are in place and/or that an Information Sharing Agreement is completed and signed by all relevant parties before information is shared with and processed by the supplier.

11. Benefits

11.1. Robust data protection practices protect the organisation from financial, reputational and operational risks. Under GDPR fines can be made up to 20 million euros or 4% or annual turnover.

11.2. Transparent processing will keep our customers and employees better informed and develop greater levels trust.

11.3. PSPS act as data processor for East Lindsey District Council, South Holland District Council, and Boston Borough Council. By complying with data protection law and demonstrating this through a thorough and properly managed Information Management Framework we reassure our client Councils that their customer and employee information is processed in a way they would reasonably expect.

12. Review

12.1. This policy should be reviewed at least once every three years to ensure that it remains fit for purpose. It may need reviewing more regularly in response to specific legislation changes or changes to best practice guidance.

12.2. The DPO retains overall responsibility for ensuring that this policy is reviewed at appropriate intervals and that it remains relevant and fit for purpose.

Appendix A – Data Breach Management Process