Appropriate Policy Document – Core Functions

Introduction

1. Purpose and context

This is the 'appropriate policy document' for IPSA that sets out how we will protect Special Categories Personal Data.

It meets the requirement at paragraph 1 of Schedule 1 to the Data Protection Act 2018 that an appropriate policy document be in place where the processing of special category personal data is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the controller or the data subject in connection with employment, social security or social protection.

It also meets the requirement at paragraph 5 of Schedule 1 to the Data Protection Act 2018 that an appropriate policy document be in place where the processing of special category personal data is necessary for reasons of substantial public interest. The specific conditions under which data may be processed for reasons of substantial public interest are set out at paragraphs 6 to 28 of Schedule 1 to the Data Protection Act 2018.

This policy explains how and why IPSA collects, processes and shares particularly sensitive personal data about data subjects in order to carry out our functions, in accordance with the data protection principles set out in the General Data Protection Regulation 2016 (GDPR.) Sensitive personal data can only be processed lawfully if it is carried out in accordance with this policy.

2. Scope

This policy applies to all IPSA functions that process Sensitive Personal Data. IPSA staff must therefore have regard to this policy when carrying out sensitive processing on behalf of the organisation.

3. References

- Data Protection Act 2018
- General Data Protection Regulation
- Human Rights Act 1998
- Freedom of Information Act 2000
- Equality Act 2010
- Employment Rights Act 1996

4. Related documents

- Information Governance and Assurance Framework
- Information Rights FOI and DPA Policy
- Information Security Policy
- Records Management Policy
- Equality and Diversity Policy
- Sickness Absence Policy

5. Responsibilities

The Data Protection Officer will have overall responsibility for this policy, ensuring organisational compliance.

6. Policy Review

This policy will be regularly reviewed and may be subject to revision. Earlier review may be required in response to relevant changes in legislation or case law, or in the event that the overarching data protection or related policies significantly change.

Policy

7. Introduction

IPSA is committed to an information governance framework that is clear and accessible, and which ensures that the collection and processing of personal data is carried out in accordance with the GDPR and the Data Protection Act 2018 (DPA).

This framework is underpinned by a scheme of delegation and a decision-making framework ensuring that data protection is explicitly considered by our staff and senior leaders, including our Senior Information Risk Owner.

IPSA values openness and transparency, and we have committed to and published a number of policies and processes to assist data subjects and to explain how we handle personal data. These include privacy notices which describe what information we hold, why we hold it, the legal basis for holding it, who we share it with, and the period we will hold it for.

IPSA has built a network of Information Asset Owners who are responsible for ensuring that the information their department collects is necessary for the purposes required and is not kept in a manner that can identify the individual any longer than necessary. They are collectively responsible for ensuring that the IPSA Information Asset Register is kept up to date and accurately reflects the information IPSA holds and the lawful basis for holding it. This network is supported by every member of staff who undertake data protection training each year.

Due to the nature of work performed at IPSA, the organisation needs to share information with other parties. IPSA has a number of Information Sharing Agreements that govern the transfer of information between parties. In addition, the IPSA Data Flow Map sets out the categories of recipients with whom information is shared.

8. The Data Protection Principles

Article 5 of the General Data Protection Regulation sets out the data protection principles. These are our procedures for ensuring that we comply with them.

(a) Principle 1

Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject. In this regard, IPSA will:

- ensure that personal data is only processed where a lawful basis applies, and where processing is otherwise lawful
- only process personal data fairly, and will ensure that data subjects are not misled about the purposes of any processing
- ensure that data subjects receive full privacy information so that any processing of personal data is transparent

(b) Principle 2

Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. IPSA will:

- only collect personal data for specified, explicit and legitimate purposes, and we will inform data subjects what those purposes are in our privacy notice

- not use personal data for purposes that are incompatible with the purposes for which it was collected. If we do use personal data for a new purpose that is compatible, we will inform the data subject first

(c) Principle 3

Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

IPSA will only collect the minimum personal data that we require for the purpose for which it is collected. We will ensure that the data we collect is adequate and relevant.

(d) Principle 4

Personal data shall be accurate and, where necessary, kept up to date.

IPSA will ensure that personal data is accurate, and kept up to date where necessary. We will take particular care to do this where our use of the personal data has a significant impact on individuals.

(e) Principle 5

Personal data shall be 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.

IPSA will only keep personal data in identifiable form as long as is necessary for the purposes for which it is collected, or where we have a legal obligation to do so. Once we no longer require personal data it shall be deleted or rendered permanently anonymous.

(f) Principle 6

Personal data shall be 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.

IPSA will ensure that there appropriate organisational and technical measures in place to protect personal data.

9. Special category data and criminal offence data

Personal data refers to any information by which a living individual can be identified. Individual identification can be by information alone or in conjunction with other information. Certain categories of personal data have additional legal protections when being processed. These categories are referred to in the legislation as “special category data” and are data concerning:

- health
- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- genetic data
- biometric data
- sex life or sexual orientation

9.1 Criminal offence data

The processing of criminal offence data also has additional legal safeguards. Criminal offence data includes information about criminal allegations, criminal offences, criminal proceedings and criminal convictions. IPSA will not ordinarily process criminal offence data.

9.2 Types of personal data we process

IPSA collects, processes and shares special category data where it is necessary in order to carry out our functions. Below is a non-exhaustive list of categories of data subjects whose personal data we process:

- MP's
- MPs' staff
- IPSA staff
- IPSA staff next of kin
- Individuals acting on behalf of other organisations
- Contractors
- Visitors to IPSA

9.3 The legal basis for processing Special Category Personal Data

As a public body it is necessary for us to process special category data in order to fulfil our functions under the Parliamentary Standards Act 2009. These functions are carried out in the public interest. We will only process it where it is necessary owing to a substantial public interest arising from maintaining public confidence in the organisation.

We also collect and retain special category data that is relevant for employment purposes (i.e. diversity and equal opportunities monitoring, as well as sickness absence and staff wellbeing). This is to ensure compliance with our duties under the Equality Act 2010.

IPSA processes Special Category Personal Data in accordance with the following provisions of the Data Protection Act 2018 and the General Data Protection Regulation:

- Article 6(1) (e) GDPR; Section 8 DPA 2018;
- Article 9(2) (b) or (g) GDPR; Section 10 and Schedule 1 Parts 1 and 2 DPA 2018.

10. Data Sharing

We are required to share personal data with third parties where we have a legal obligation to do so. We may also share information with other public bodies (such as the House of Commons), and government departments in order to facilitate the exercise of their statutory or other public functions.

11. Data Subjects' Rights

Data Protection legislation affords Data Subjects a number of rights relating to their personal data, including Special Category Personal Data. These rights are subject to some specific exemptions. Data Subjects' rights include:

- the right of access
- the right to rectification
- the right to restrict processing
- the right to object to processing
- the right to erasure
- the right to be notification
- rights relating to automated decision making and data portability

12. Data Controller and Data Protection Officer

IPSA's data controller is the Accounting Officer. The data controller has overall control of the purpose for which and the manner in which IPSA obtains and processes personal data, and who must ensure that this is done in accordance with the data protection principles.

IPSA also has a designated Data Protection Officer as well as a Freedom of Information and Policy Team. The Data Protection Officer is responsible for:

- facilitating data subject rights and making key decisions such as to whether the applicant has a right to access the data requested
- supporting the SIRO Group meetings, chaired by the organisation's SIRO
- leading cooperation with the Information Commissioner's Office for the organisation
- deciding whether a data protection impact assessment is needed where a change in business processes is proposed and advising to ensure compliance with relevant data protection laws
- responding to concerns from the public in relation to how IPSA processes personal data
- advising whether any proposed information sharing agreement would be data protection compliant

- carrying out investigations into any data breach within the organisation and recommending appropriate changes to ensure best practice methods are adhered to
- providing independent advice to the organisation on its data protection obligations

13. Information Security

IPSA deploys a wide range of Technical and Procedural controls in order to protect the personal data it holds and processes.

Controls include but are not limited to:

- Mandatory annual Information Security Training for all staff
- Acceptable use of IT equipment and systems defined in Security Operating Procedures signed by all users of IPSA systems
- Role Based Access Controls, limiting IPSA system users to only access those systems necessary for them to perform their duties
- Identity and Access Management through Human Resources hiring and reference polices, including HMG Security Clearances.
- Strong defences of IPSA core IT system (e.g. Firewalls, Malware Detection & Defence)
- Monitoring and / or logging of digital and user activity into, within and out of IPSA systems
- Robust procedures for the reporting of any data or potential data breaches.

IPSA continuously reviews and upgrades these controls as part of ongoing security improvement plans, to maintain the security of our systems and to protect the information that we hold.

Document history

Title:	Appropriate Policy Document – Core Functions
Original author(s):	Data Protection Officer
Owner:	SIRO
Reviewed by:	SIRO Group
Approval body:	SIRO Group
Approval date:	30 November 2018
Review frequency:	Annual
Next review date:	October 2019

Version	Date	Status	Update by	Comment
1.0	30/11/2018	Approved	Anthony Palmos	Approved
1.1	02/10/2020		Data Protection Officer	Rebrand