SPCB Corporate Data Protection Policy

Introduction

The SPCB is fully committed to compliance with the requirements of the General Data Protection Regulation (the GDPR) which came into force on 25 May 2018 and the Data Protection Act 2018 (the DPA).

The SPCB will follow procedures and best practice which aim to ensure that all employees, MSPs and their staff, suppliers, clients, customers, advisers and visitors to Holyrood are fully aware of our duties in line with these requirements in relation to normal and special categories of personal data and that the rights of all data subjects set out in the GDPR are clearly set out, transparent and are fully evidenced and auditable.

The SPCB will ensure that the rights of data subjects set out in the GDPR are met.

The SPCB is a data controller and a data processor. As a data controller the SPCB undertakes to satisfy its duties with regard to its activities as a data controller and as a data processor and these are set out in detail in this policy.

Statement of policy:

As a data controller the Scottish Parliament and Scottish Parliamentary Corporate Body must collect and use certain types of information about individuals with whom it interacts. These may include for example current, past and prospective employees, MSPs and their staff, clients and customers, expert witnesses and advisers and others with whom it communicates. comprehensive In addition it may be required to collect and use information in order to comply with the requirements of democratic processes. Comprehensive information regarding personal data processing undertaken by the SPCB are set out in our corporate privacy notice here (add link).

The SPCB will process all personal data according to the requirements of the GDPR and the DPA however it is collected, recorded and used, irrespective of its format and including for example paper copies, computer records, datasets, and data held on applications and devices.

The SPCB understand that privacy by design and the lawful and correct treatment of personal information as central to its successful operations and to maintaining confidence between the SPCB and those with whom we interact. We ensure that our organisation processes all personal data in a way that is lawful and correct and we fully endorse and adhere to the Principles set out in the GDPR.

As a data processor, the SPCB undertakes to inform all stakeholders including MSPs of its obligations in relation to this activity which will be carried out and regularly reviewed in line with GDPR requirements.

Who to contact: Claire Turnbull, Head of Information Governance and Data Protection Officer

Email: claire.turnbull@parliament.scot

Telephone: 0131 348 6913

Background

The General Data Protection Regulation (GDPR) regulates and protects the processing of personal data about individuals by using the law to protect our data and the way it is used by third parties and by recognising that personal data is a valuable asset which must be safeguarded and actively managed.

Article 5 of the GDPR requires that personal data shall be:

"a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) 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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f) 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."

Article 5(2) requires that:

"the controller shall be responsible for, and be able to demonstrate, compliance with the principles."

GDPR Principles:

Article 5 of the GDPR requires that personal data shall be:

"a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) 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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f) 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."

Article 5(2) requires that:

"the controller shall be responsible for, and be able to demonstrate, compliance with the principles."

In order to meet the data protection principles set out in the GDPR the SPCB will:

- Fully observe the conditions regarding the fair collection and use of personal data.
- Meet its legal obligations to specify the purposes for which information is collected and used.
- Collect and process personal data only to the extent that it is required to fulfil operational purposes or to comply with legal requirements.

- Put in place adequate processes to ensure the quality of data.
- Hold personal data on our systems only for the length of time necessary to fulfil our operational purposes and in line with our corporate records retention schedule.
- Ensure all the rights of the individuals about whom we hold data can be fully exercised.
- Take all appropriate technical and organisational security measures to safeguard personal data. 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."
- Ensure that personal data held by the SPCB is not transferred to areas outside the EEA without appropriate safeguards.

In addition, the SPCB will ensure that:

- Privacy by design is satisfied and that data protection impact assessments are undertaken and regularly reviewed for all activities, projects and engagement requiring personal data processing.
- A Data Protection Officer is in place whose work is adequately supported and resourced.
- GDPR roles and responsibilities are set out clearly and regularly reviewed.
- Information about how it processes personal data is set out in a corporate privacy notice and that this is regularly maintained and updated.
- It has suitable accountability processes in place and can provide auditable tracking of personal data collected and held.
- The legal basis for processing personal data is understood and applied to all the types of personal data it collects and stores.
- Where consent is the legal basis for processing, auditable evidence of processing is satisfied.
- When the SPCB engages with external groups to seek information or to circulate surveys or newsletters, all subscribers will have a clear opportunity to unsubscribe.
- All SPCB staff and contractors undertake regular mandatory training on GDPR requirements and that the SPCB can provide evidence of this.

- This policy is available to each SPCB employee and complying with it is part of the terms and conditions of employment.
- Clear, up to date information about data protection requirements is available to all of our staff.
- Everyone managing and handling personal data is appropriately trained and supervised.
- Enquiries about handling personal data meet the rights of individuals set out in the GDPR and are promptly and courteously handled.
- Methods and performance of handling personal data are regularly assessed and evaluated.
- All MSPs (who are individual data controllers in their own right) and their staff are provided with suitable guidance in handling personal data.
- All contractual arrangements with third parties who process personal data on behalf of the SPCB are required to provide regular evidence of compliance with GDPR requirements.
- The Head of Information Governance and Data Protection Officer reports regularly to the Leadership Group which approves all changes to this policy.

<u>The rights of data subjects:</u>

The GDPR provides the following rights for individuals:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling
9. Increased rights for children over the age of 13

In order to meet these rights, the SPCB will:

- Clearly set out the rights of individuals on its corporate privacy notice.
- Ensure that all staff and contractors are aware of these rights and understand how they must be met.
- Have suitable processes and procedures in place to meet individual rights.

<u>Security of personal data:</u>

- The SPCB recognises that individuals choose to share their personal data with our organisation and that we must ensure that we have sufficient technical and organisational measures in place to safeguard that personal data appropriate to its content including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage by using appropriate technical or organisational measures. For this reason any disclosure of personal data gathered by its staff or contractors during the course of their employment or assisting other to do so is viewed by the SPCB with the utmost seriousness.

- The SPCB has put in place a data breach framework as part of its business continuity management processes to mitigate against the effects of any data breach which includes the requirement to notify the office of the ICO of any breach with 72 hours.

Information and computer security

All SPCB employees must comply with the guidance and standards set out in the Computer Security Policy and the Acceptable Use of IT Policy

http://www.parliament.scot/intranet/16251.aspx

http://www.parliament.scot/31563.aspx

The Scottish Parliament website and cookies

The Scottish Parliament website uses Google Analytics

- to gather information about how visitors use our website to help us improve its performance

- to improve the visitor experience when using our website by delivering pages more quickly or remembering user settings.

The information we collect is anonymous and it cannot identify an individual.

http://www.scottish.parliament.uk/help/46282.aspx

Data Protection Notification:

The SPCB is listed on the public register of data controllers maintained by the UK Information Commissioner and undertakes to renew its notification every 12 months. The Head of Information Governance is responsible for annual data protection notification on behalf of the SPCB and she will review the data protection notification regularly. Any changes to the register will be notified to the Commissioner within 28 days.

Date	Version	Summary of changes
30/04/2018	1.0	