


## Group Standard

# Information & Data Privacy

A man in a blue t-shirt with the Serco logo and "FIRE & RESCUE" text is pointing upwards with his right hand towards a large graphic. The graphic consists of two concentric red circles. The text is centered within the inner circle.

Serco recognises the importance of effective information, document and record management in order to enable effective decision making and of ensuring any information produced, or any personal data processed, meets customer, legislative and regulatory requirements

## Document Details

Document Details	Serco Business
<b>Reference</b> SMS GS-II1	<b>Version</b> 2.1
<b>Approval Date</b> June 2020	<b>Date for next review</b> June 2022
<b>Applicability</b> Serco Group covering all business regions, operating companies and business units throughout the world <sup>1</sup> covering: <ul style="list-style-type: none"> <li>- employees, officers, directors and individuals working as consultants and contractors and any other parties acting as representatives or agents of Serco (Employees)</li> <li>- wholly owned subsidiaries and majority-owned operations</li> </ul> Where a minority interest and in regard to its subcontractors and suppliers Serco encourages alignment with this Standard	
<b>Authority</b> Chief Executive, Serco Group plc	
<b>Accountable Policy Owners (Group)</b> Chief Information Officer (Group)	
<b>Additional Information</b> Supporting standards, standard operating procedures and guidance relating to this Group Standard are available within the Serco Management System	
<b>Governance</b> Our policies and standards, together with any regional or market requirements and enhancements to them, are authorised through a robust governance process.	
<b>Consequence Management</b> As a Group Standard the requirements detailed in this document are mandated and must be adhered to. Non-compliance will have consequences which may include disciplinary action. The Consequence Management Group Standard (SMS-GS-G1) details how instances of non-compliance will be dealt with	
<sup>1</sup> As used herein, Serco Group plc and its affiliates, subsidiaries, business units/divisions, joint venture companies and operating companies are referred to as 'Serco', 'Company'/ 'company', 'we', 'us' or 'our'.	

## Contents

1 Objectives .....	2
2 Policy Standards .....	2
2.1 Data management .....	2
2.2 Personal data protection requirements .....	3
2.2.1 Personal Data Protection Impact Assessments.....	4
2.2.2 Personal Data Inventory .....	4
2.2.3 Privacy by Design .....	4
2.2.4 High Risk Data Privacy Guidance .....	4
2.3 Contract document management .....	4
2.4 Incident reporting – personal data breach .....	5
2.5 Freedom of information .....	5
2.6 Document and record management and retention.....	6
3 Responsibilities & Accountabilities .....	7
4 Processes and Controls.....	9
4.1 Governance processes and controls.....	9
4.2 Key processes and controls.....	16
5 Supporting documentation and guidance .....	23
6 Definitions .....	23
7 Further information and support .....	24

# 1 Objectives

---

**Serco recognises its responsibility to ensure that any information produced, or any personal data processed, meet customer, legislative and regulatory requirements and is accurate, kept up to date, consistent and provided in a timely manner in order to enable effective decision making.**

To achieve this we will:

- demonstrate data and information integrity internally, externally and with our customers by providing accurate, kept up to date, consistent and timely responses
- ensure personal data is handled in line with customer, legislative and regulatory requirements, and relevant Serco privacy-related policy standards and operating procedures<sup>2</sup>
- not make misleading, false or exaggerated claims concerning the Company, or competitors
- mandate and monitor acceptable use standards regarding employees' access, processing and publishing of information (including the use of social media)<sup>3</sup>
- manage the access to information available on Our World, the Company's intranet, and ensure that persons authorised to process personal data are reliable and under an appropriate obligation of confidentiality
- classify information in accordance with the Security Group Standard<sup>4</sup>
- ensure that the principles of data protection by design and by default are taken into consideration when processing personal data
- record all commercial, business and legal transactions and securely maintain all material documents, including signed contract documents and variations
- ensure consistency of response and accurate reporting of incidents and accidents<sup>5</sup>

- manage requests for information from public authorities and data subjects in accordance with local regulations, all applicable data protection laws and requirements
- only retain personal data, documents and records in accordance with business and legislative requirements or in compliance with a legal obligation, ensuring storage and retrieval costs are minimised
- implement effective document management processes and controls to ensure all documents and records (including those containing personal data) are handled, processed, retained and disposed of appropriately<sup>6</sup>

## 2 Policy Standards

---

### 2.1 Data management

- S1. When providing information internally or externally, or responding to customer enquiries, tenders and bids as well as media, regulatory agencies and other external audiences, the information issued on behalf of the Company will be accurate, consistent, complete and timely. We will not make misleading, false or exaggerated claims concerning the Company, or competitors
- S2. All business information of Serco will be treated with confidentiality, including information obtained regarding Serco's customers and other business partners
- S3. Sensitive information will be protected by appropriate confidentiality agreements and applicable security protocols and encryption, distinguished from information that is freely disclosable and clearly marked<sup>7</sup>
- S4. All information created on the internet or other social media will be fair to and respect all religions, political, economic and racial differences and opinions and show proper consideration for others' privacy

<sup>2</sup> See section 6 for a list of all applicable Serco policy standards and operating procedures.

<sup>3</sup> See Acceptable Use of Information Systems Group Standard Ref: SMS-GS-BC1

<sup>4</sup> See Security Group Standard Ref: SMS-GS-S1

<sup>5</sup> See Incident & Fraud Reporting & Management GSOP Ref: SMS GSOP O1-2

<sup>6</sup> See Data Retention GSOP Ref: SMS GSOP II1-2

<sup>7</sup> See Acceptable Use of Information Systems Group Standard (Privacy) Ref: SMS-GS-BC1

- S5. Customer information will remain confidential unless the customer has given written consent, or the Divisional Legal Representative has confirmed that the law or the contract requires its disclosure
- S6. All employees will ensure that the information they access, process and publish which relate to Serco (whether in or outside of work) comply with:
- our Values
  - our Code of Conduct
  - relevant Serco policy standards and operating procedures
  - all applicable laws (including copyright, trademarks, the fair use of material owned by others and data protection legislation), and do not result in harm or damage to Serco's reputation
- S7. Financial records and reports will be accurate and complete and will conform to relevant international and national legislation and regulations<sup>8</sup>
- S8. Internal and external performance and compliance information will be verifiably accurate. If this information cannot be verified, this should be noted when the information is reported. An action plan will be developed to ensure information can be verified as accurate in the future. If this is not possible then the issue will be reported to the next level of management
- S9. Serco employees will not falsify records or misrepresent facts
- S10. Material which refers to Serco or uses the Company's name on multi-media and social networking websites may be published, provided that this is done in a professional and responsible manner, does not harm or tarnish the image, reputation and goodwill of Serco and our employees and meets our Acceptable Use of Information Systems Group Standard<sup>9</sup>
- S11. Where mistakes occur in the provision of information, these must be corrected in a timely manner

## 2.2 Personal data protection requirements

- S12. Serco will provide assistance to our customers to comply with data protection obligations relating to the personal data they collect (and we process) (i.e. data subject rights requests)
- S13. Serco will meet data protection obligations in relation to the personal and sensitive data we collect (i.e. from our employees and members) and all employees and business partners will process any personal data in compliance with:
- all applicable contractual requirements
  - relevant Serco Data Privacy policy, standards and operating procedures<sup>10</sup>
  - all applicable data privacy laws and regulations
- S14. Data Inventories will be maintained containing details of business processes which use personal data<sup>11</sup>. Processes will also be implemented that ensure our business partners maintain similar data inventories in relation to the personal data they process on our behalf<sup>12</sup>
- S15. Appropriate technical and organisational security measures will be taken to prevent unauthorised or unlawful disclosure or access to, or accidental or unlawful loss, destruction, alteration or damage to personal data<sup>13</sup>
- S16. Personal data will only be disclosed outside of Serco to third parties where there:
- is a contractual requirement to do so;
  - is written consent from our customer to do so;
  - is a legitimate business need; or
  - is a legal obligation to disclose.

Particular care will be taken when transferring personal data overseas. For example, restrictions are often imposed regarding the transfer of personal data outside of the United Kingdom due to customer requirements<sup>14</sup>

<sup>8</sup> See Finance Group Standard Ref: SMS-GS-F1

<sup>9</sup> See Acceptable Use of Information Systems Group Standard Ref: SMS-GS-BC1

<sup>10</sup> See footnote 2 above

<sup>11</sup> The Data inventory is part of the Data Protection Toolkit

<sup>12</sup> See Procurement and Supply Chain Group Standard Ref: SMS-GS-PSC1

<sup>13</sup> See Security Group Standard Ref: SMS-GS-S1 & Information Integrity Policy Ref: SMS-PS-II

<sup>14</sup> See Data Protection GSOP Ref: SMS-GSOP-S1-3.

- S17. Data subject rights requests will be dealt with where there is a contractual obligation to do so or when requested, and as instructed, by our customers
- S18. Our customers may ask us, or we may be under a contractual obligation, to assist them to comply with data subject rights requests they receive from their data subjects. In these situations, we will act on the instructions of our customers.
- S19. Where Serco receives data subject right requests from a data subject, such as an employee, these requests will be handled in accordance with relevant and appropriate Serco procedures. Time limits for responding to data subject rights requests will be met

## 2.2.1 Personal Data Protection Impact Assessments

- S20. A Data Protection Impact Assessment (DPIA)<sup>15</sup> will be carried out to identify and mitigate privacy risks and apply the principles of 'privacy by design' where a new project, system, technology solution or way of working or changes are proposed to an existing project, system, technology solution or way of working involving intensive or higher risk processing of personal or sensitive personal data

## 2.2.2 Personal Data Inventory

- S21. All Contracts and Functions will produce a Data Inventory at business activity level e.g. activities which may cut across multiple departments. This Data Inventory will maintain a record of personal data processing activities within business activities where personal data is processed. The Data Inventory will establish a record of the data that is processed, the process for which each category of personal data is used, related data processing risks, how it is stored and with whom it is shared
- S22. The Data Inventory will be produced and maintained by the local Data Protection Champion or under their supervision and stored in a Data Protection Register. The Data Inventory will be reviewed as required and as a minimum where material changes occur within the Contract/Function

## 2.2.3 Privacy by Design

- S23. 'Privacy by design' will be used as an approach to projects to promote data protection compliance from the start. This approach will help Serco comply with its obligations under Data Protection legislation and will be a key consideration in the early stages of any project, and then throughout its lifecycle. For example when:
- building new IT systems for storing or accessing personal data;
  - developing legislation, policy or strategies that have privacy implications;
  - embarking on a data sharing initiative; or
  - using data for new purposes.

## 2.2.4 High Risk Data Privacy Guidance

- S24. The identification of high risk Contracts/Functions/processing activities will be undertaken to prioritise data privacy/protection risks and the identification of activities and actions required to manage and/or mitigate those risks
- S25. A DPIA will be completed where data processing is likely to result in a high risk to the rights and freedoms of 'natural persons'
- S26. Data Protection Champions will provide advice and support regarding the classification of data privacy/protection risks and the prioritisation of whether a DPIA is required

## 2.3 Contract document management

- S27. All commercial, business and legal transactions, including information relating to contract change, contractual negotiation, financial and service performance, will be properly and accurately recorded with input from the Divisional Legal Representative
- S28. All material documents that govern Serco's contractual relationships, including signed contract documents and variations, must be held in a safe and secure manner and in accordance with data retention requirements<sup>16</sup>

<sup>15</sup> See Data Protection Impact Assessment GSOP Ref: SMS-GSOP-II1-3

- S29. Where contractual documentation is stored electronically it must be securely stored on a Serco managed network with adequate security controls (as required by the security classification)<sup>17</sup>
- S30. Where documents are stored on a customer network, and there is no secondary store in a Serco managed network, a document register must be maintained, stating document location and access methods, to ensure information is accessible by Serco employees
- S31. Where contractual documentation must be retained in hard-copy format, this must be stored in appropriately secured file storage location on Serco premises, on a contract site or at an approved 3rd party archive location
- S32. Hard copy documents must be recorded in a document register that is stored within the contract's electronic document management system
- S33. A clear audit trail of contractual documents and their changes will be maintained to preserve commercial and contractual integrity during the lifetime of service delivery and beyond. All documents must be clearly marked with a version number and provide a change history
- S34. It is recognised that Contracts relating to Government secure or restricted goods or services may implement additional security requirements, which will impact on the nature of both the physical and electronic locations for document storage and access to this storage. Where such requirements are in place, they will be complied with
- S35. Contracts and other documents relating to a contractual dispute or claim (for instance internal and external correspondence) will be maintained and not released or destroyed except as directed by Serco's legal representatives

## 2.4 Incident reporting – personal data breach

- S36. All personal data breaches will be captured, categorised and reported in accordance with defined procedures and all breaches or suspected breaches will be immediately reported to the data controller who will determine the nature, severity and level of risk associated with the breach/suspected breach<sup>18</sup>
- S37. All personal data breaches/suspected breaches will also be immediately reported to the relevant line manager and to the Data Protection Champion to ensure that any breach or suspected breach is known and that appropriate advice and actions are taken
- S38. All personal data breaches or suspected breaches will be categorised and reported using the Serco Incident Reporting Scale (SIRS), subject to any applicable limitations, e.g. confidential reporting and other regulated activity, and in a manner so as to properly preserve defences, legal privileges and other rights and interests of Serco<sup>19</sup>
- S39. All data breaches will be contained and remedied as soon as possible, and where necessary all appropriate stakeholders, including customers, will be informed of the data breach
- S40. All personal data breaches will be recorded on ASSURE and reported to any other appropriate national or other regulatory body in accordance with legal requirements
- S41. Corrective and preventive actions will be implemented and communicated following investigations known or suspected personal data breaches

## 2.5 Freedom of information

- S42. Processes will be in place to handle requests for information by the public where there is a statutory or regulatory requirement to do so. In the UK this relates to the Freedom of Information Act 2000 and the Environment Information Regulation 2004<sup>20</sup>

<sup>16</sup> See Document Retention GSOP Ref: SMS-GSOP-III-2

<sup>17</sup> See Security Group Standard Ref: SMS-GS-S1

<sup>18</sup> See Incident & Fraud Reporting & Management GSOP Ref: SMS-GSOP-O1-2

<sup>19</sup> SIRS is detailed in Annex A of Incident & Fraud Reporting & Management GSOP Ref: SMS-GSOP-O1-2

<sup>20</sup> See Freedom of Information GSOP Ref: SMS GSOP II1-1



- S43. Where such requests are made, Serco will work with the customer to ensure an appropriate and proportionate response
- S44. Any information that is published must not compromise personal security of the individual, their colleagues, our customers or our business. Particular care must be taken regarding government or public sector clients; in these cases vetting status or the sensitivity of the work being done must not be disclosed
- S45. All commercially sensitive, trade secrets or confidential information will be clearly marked in accordance with information privacy classification procedures<sup>21</sup>

## 2.6 Document and record management and retention

- S46. Documents and records can be held on behalf of our customers and on our own behalf and will be handled, retained and disposed of, appropriate to their security classification, document type, retention period<sup>22</sup> and, where such documents/records, contain personal data, in accordance with applicable legislative and regulatory requirements
- S47. Except for any customer-specific document management/retention requirements, all documents and records will be managed in accordance with Data Retention<sup>23</sup> and Information Privacy Classification procedures in the Group Security Manual<sup>24</sup>
- S48. Documents and records handled and stored on behalf of our customer (but not owned by Serco) will be managed in line with customer contractual requirements
- S49. Data retention systems and procedures will be established which address the manner in which the particular organisation and employees deal with documents in the various jurisdictions they operate within
- S50. Procedures will be implemented for the retention and destruction of hard and soft copies of documents created and received by Serco

- S51. Records will be kept for as long as is necessary for the business purposes of Serco which may be defined in legislation, regulatory or contractual requirements. Other circumstances may also need to be considered such as litigation, government investigation or those identified by the Divisional Legal Representative or their designee(s)
- S52. Where the Divisional Legal Representative has identified a need to retain records, they will notify appropriate departments and retain relevant records until further notice, ensuring disposal of those records when no longer required in an appropriate manner and timeframe
- S53. Document ownership will be clearly defined where operating procedures or supporting documentation are shared with the customer. Such documents will be appropriately identified and classified to ensure the correct Intellectual Property Rights and Data Classification status are established as defined

<sup>21</sup> See Information Privacy Classification section of Security Manual Ref: SMS GSOP-S-SECMAN

<sup>22</sup> See Security Group Standard Ref: SMS-GS-S1

<sup>23</sup> See Data Retention GSOP Ref: SMS GSOP II1-2

<sup>24</sup> See Information Privacy Classification section of Security Manual Ref: SMS GSOP-S-SECMAN

### 3 Responsibilities & Accountabilities

S54. The following responsibilities will apply to the delivery of the defined standards. If these are not completed effectively, the person responsible will be accountable for any consequences<sup>25</sup>.

#### Group

S55. The Group CEO will ensure that data protection processes and resources are in place to ensure compliance with data protection legislation requirements globally.

S56. The Group CEO will appoint an accountable person who will be globally responsible for data protection. This person may perform other operational tasks in addition to this role, as no legal conflict of interest rules would apply. This role will be responsible for:

- a. ensuring there is alignment across the global business for data protection
- b. working with (Divisional) Data Protection Officers (DPOs) (who would be advisors) to set strategy and ensure data related policy is properly executed operationally
- c. informing and advising Serco of its obligations relating to the processing of personal data in accordance with applicable data protection/privacy laws and regulations

#### Division

S57. The Divisional CEO/Corporate Shared Services (CSS) MD will appoint a Data Protection Officer(s) (DPO) reporting directly to the Group General Counsel, with responsibility for:

- a. ensuring that data protection processes and resources are in place to ensure compliance with data protection policy, standards and processes and with data protection legislation
- b. implementing Information and Data Management policy, standards, procedures and key controls across the Division/CSS; which may include the development of country/region/Divisional procedures and management systems

- c. ensuring appropriate Information and Data Management resources are available to support the business
- d. ensuring appropriate training is available and provided
- e. implementing a management assurance framework to provide confidence that key controls are being implemented effectively
- f. monitoring the compliance of Serco with applicable data protection/privacy laws and regulations
- g. providing advice on and monitoring the undertaking of, data protection impact assessments (DPIAs)
- h. co-operating with relevant supervisory authorities
- i. acting as the point of contact for relevant supervisory authorities in relation to issues concerning the processing of personal data
- j. overseeing the handling of data subject rights requests received within the Division/CSS
- k. acting as the point of contact for all employees within the Division/CSS in relation to all data protection and privacy related matters
- l. providing oversight and reporting data protection and privacy performance
- m. providing regular reports to Group on all data protection and privacy related matters
- n. notifying Group immediately upon becoming aware of any loss or suspected loss of personal data or breach of Serco data protection/privacy-related policy standards and operating procedures

#### Business Unit

S58. The Business Unit Managing Director is responsible for:

- a. ensuring Data Protection/Privacy and Information and Data Management requirements are implemented across the Business Unit
- b. ensuring appropriate processes and controls are implemented and effective across their Business Unit
- c. ensuring appropriate processes and controls are implemented and effective with all joint venture partners

<sup>25</sup> See Consequence Management Group Standard Ref: SMS-GS-G1



**Contract/Functional Areas**

S59. Contract Managers/Functional area leads are responsible for appointing a Data Protection Champion in areas where there are personal data management activities and risks

S60. Contract Managers/Functional Areas are accountable for:

- a. ensuring that Data Protection/Privacy and Information and Data Management responsibilities are clearly defined and appropriate controls are in place
- b. providing assurance that these requirements are being implemented effectively
- c. ensuring training is provided and recorded to identified data handlers and data owners (in particular those handling personal data) to ensure they understand local processes, roles and responsibilities
- d. ensuring all records and documentation (including contractual documentation) are held in a safe and secure manner and in accordance with document management and Data Retention requirements<sup>26</sup>
- e. liaising with the Divisional/CSS DPO for advice and guidance, where required, regarding data and information retention, security and disclosure
- f. ensuring all incidents breaches and suspected breaches (in particular those concerning any loss of personal data) are managed in accordance with Incident & Fraud Reporting and Management procedures<sup>27</sup> and reported into ASSURE within defined timescales and categorised according to SIRS

- d. immediately reporting any loss of personal data or breach of Serco's data protection/privacy-related policy standards or operating procedures to their line manager, local Data Protection Champion and/or Divisional DPO, in accordance with local processes and the Incident & Fraud Reporting and Management GSOP<sup>28</sup>
- e. immediately reporting receipt of a data subject rights/request, such as a subject access request to the subject access team in accordance with local/Divisional/Country procedures and notifying the local Data Protection Champion and /or Divisional DPO
- f. promptly informing a line manager or local Data Protection Champion and/or Divisional DPO of any information or data management concerns

**All employees**

S61. All employees are responsible for:

- a. understanding and following Serco's Code of Conduct at all times
- b. understanding and complying with all applicable Serco policy standards, operating procedures, defined work instructions, method statements and risk assessments
- c. undertaking training provided and ensuring any mandatory training is kept up to date

<sup>26</sup> See Data Retention GSOP Ref: SMS GSOP II1-2

<sup>27</sup> See Incident & Fraud Reporting & Management GSOP Ref: SMS GSOP O1-2

<sup>28</sup> See Incident & Fraud Reporting & Management GSOP Ref: SMS GSOP O1-2

# 4 Processes and Controls

## 4.1 Governance processes and controls

### Process

A set of related activities that must be carried out to achieve policy outcomes

### Controls

The action we put in place to mitigate a risk(s) within a key process and/or the delivery of policy outcomes. These are mandated and are the minimum that should be implemented regardless of any local difference

### Responsibility

for ensuring controls are in place and operating effectively

Ref	Description	Ref	Description	Group (S55 & S56)	Division (S57)	Business Unit (S58)	Contract (S59 & S60)	All Employees (S61)
P1	Responsibilities are defined and understood	↔ C1	<p>A Group data protection lead is appointed by the Group CEO with responsibility for:</p> <ul style="list-style-type: none"> <li>ensuring there is alignment across the global business for data protection</li> <li>working with (Divisional) Data Protection Officers (DPOs) (who would be advisors) to set strategy and ensure data related policy is properly executed operationally</li> <li>informing and advising Serco of its obligations relating to the processing of personal data in accordance with applicable data protection/privacy laws and regulations</li> </ul>	●	○	○	○	○
		↔ C2	<p>A Divisional Data Protection Officer(s) is appointed with responsibility for:</p> <ul style="list-style-type: none"> <li>ensuring that data protection processes and resources are in place to ensure compliance with data protection policy, standards and processes and with data protection legislation</li> </ul>	○	●	○	○	○

**Process**

A set of related activities that must be carried out to achieve policy outcomes

**Controls**

The action we put in place to mitigate a risk(s) within a key process and/or the delivery of policy outcomes. These are mandated and are the minimum that should be implemented regardless of any local difference

**Responsibility**

for ensuring controls are in place and operating effectively

**Ref Description**

**Ref Description**

**Group (S55 & S56)**  
**Division (S57)**  
**Business Unit (S58)**  
**Contract (S59 & S60)**  
**All Employees (S61)**

- implementing Information and Data Management policy, standards, procedures and key controls across the Division/CSS; which may include the development of country/region/Divisional procedures and management systems
- ensuring appropriate Information and Data Management resources are available to support the business
- ensuring appropriate training is available and provided
- implementing a management assurance framework to provide confidence that key controls are being implemented effectively
- monitoring the compliance of Serco with applicable data protection/privacy laws and regulations
- providing advice on and monitoring the undertaking of, data protection impact assessments (DPIAs)
- co-operating with relevant supervisory authorities
- acting as the point of contact for relevant supervisory authorities in relation to issues concerning the

**Process**

A set of related activities that must be carried out to achieve policy outcomes

**Controls**

The action we put in place to mitigate a risk(s) within a key process and/or the delivery of policy outcomes. These are mandated and are the minimum that should be implemented regardless of any local difference

**Responsibility**

for ensuring controls are in place and operating effectively

**Ref Description**

**Ref Description**

**Group (S55 & S56)**  
**Division (S57)**  
**Business Unit (S58)**  
**Contract (S59 & S60)**  
**All Employees (S61)**

- overseeing the handling of data subject rights requests received within the Division/CSS
- acting as the point of contact for all employees within the Division/CSS in relation to all data protection and privacy related matters
- providing oversight and reporting data protection and privacy performance
- providing regular reports to Group on all data protection and privacy related matters
- notifying Group immediately upon becoming aware of any loss or suspected loss of personal data or breach of Serco data protection/privacy-related policy standards and operating procedures

➔ C3

- Business Unit MDs are responsible for:
- ensuring Data Protection/Privacy and Information and Data Management requirements are implemented across the Business Unit
  - ensuring appropriate processes and controls are implemented and effective across their Business Unit

○ ○ ● ○ ○

**Process**

A set of related activities that must be carried out to achieve policy outcomes

**Controls**

The action we put in place to mitigate a risk(s) within a key process and/or the delivery of policy outcomes. These are mandated and are the minimum that should be implemented regardless of any local difference

**Responsibility**

for ensuring controls are in place and operating effectively

**Ref Description**

**Ref Description**

**Group (S55 & S56)**  
**Division (S57)**  
**Business Unit (S58)**  
**Contract (S59 & S60)**  
**All Employees (S61)**

ensuring appropriate processes and controls are implemented and effective with all joint venture partners

→ C4

Contract Managers/Functional area leads are responsible for:

- appointing a Data Protection Champion in areas where there are personal data management activities and risks
- ensuring that Data Protection/Privacy and Information and Data Management responsibilities are clearly defined and appropriate controls are in place
- providing assurance that these requirements are being implemented effectively
- ensuring training is provided and recorded to identified data handlers and data owners (in particular those handling personal data) to ensure they understand local processes, roles and responsibilities
- ensuring all records and documentation (including contractual documentation) are held in a safe and secure manner and in accordance with document management and Data Retention requirements

○ ○ ○ ● ○

**Process**

A set of related activities that must be carried out to achieve policy outcomes

**Controls**

The action we put in place to mitigate a risk(s) within a key process and/or the delivery of policy outcomes. These are mandated and are the minimum that should be implemented regardless of any local difference

**Responsibility**

for ensuring controls are in place and operating effectively

**Ref Description**

**Ref Description**

**Group (S55 & S56)**  
**Division (S57)**  
**Business Unit (S58)**  
**Contract (S59 & S60)**  
**All Employees (S61)**

- liaising with the Divisional/CSS DPO for advice and guidance, where required, regarding data and information retention, security and disclosure
- ensuring all incidents breaches and suspected breaches (in particular those concerning any loss of personal data) are managed in accordance with Incident Reporting and Management procedures and reported into ASSURE within defined timescales and categorised according to SIRS

↔ C5

- All employees are responsible for:
- understanding and following Serco's Code of Conduct at all times
  - understanding and complying with all applicable Serco policy standards, operating procedures, defined work instructions, method statements and risk assessments
  - undertaking training provided and ensuring any mandatory training is kept up to date
  - immediately reporting any loss of personal data or breach of Serco's data protection/privacy-related policy standards or operating procedures to

○ ○ ○ ○ ●



### Process

A set of related activities that must be carried out to achieve policy outcomes

### Controls

The action we put in place to mitigate a risk(s) within a key process and/or the delivery of policy outcomes. These are mandated and are the minimum that should be implemented regardless of any local difference

### Responsibility

for ensuring controls are in place and operating effectively

#### Ref Description

#### Ref Description

**Group (S55 & S56)**  
**Division (S57)**  
**Business Unit (S58)**  
**Contract (S59 & S60)**  
**All Employees (S61)**

Ref	Description		Ref	Description	Group (S55 & S56)	Division (S57)	Business Unit (S58)	Contract (S59 & S60)	All Employees (S61)
				their line manager, local Data Protection Champion and/or Divisional DPO, in accordance with local processes and the Incident Reporting and Management GSOP <ul style="list-style-type: none"> <li>immediately reporting receipt of a data subject rights/request, such as a subject access request to the subject access team in accordance with local/Divisional/Country procedures and notifying the local Data Protection Champion and /or Divisional DPO</li> <li>promptly informing a line manager or local Data Protection Champion and/or Divisional DPO of any information or data management concerns</li> </ul>					
P2	Establish Information & Data Privacy policy	➔	C6	Policy, standards and Group procedures are defined and published	●	○	○	○	○
		➔	C7	Policy, standards and Group procedures are communicated and implemented	●	●	●	●	○
P3	Establish Information and Data Privacy systems and processes	➔	C8	Information and Data Privacy Procedures are defined, implemented and communicated	●	●	●	●	○

**Process**

A set of related activities that must be carried out to achieve policy outcomes

**Controls**

The action we put in place to mitigate a risk(s) within a key process and/or the delivery of policy outcomes. These are mandated and are the minimum that should be implemented regardless of any local difference

**Responsibility**

for ensuring controls are in place and operating effectively

**Ref Description**

**Ref Description**

**Group (S55 & S56)**  
**Division (S57)**  
**Business Unit (S58)**  
**Contract (S59 & S60)**  
**All Employees (S61)**

Ref	Description	Ref	Description	Group (S55 & S56)	Division (S57)	Business Unit (S58)	Contract (S59 & S60)	All Employees (S61)
		↻ C9	Legal and regulatory Information and Data Privacy requirements are monitored with changes reflected in systems, procedures and work instructions	●	●	●	●	○
P4	Information and Data Privacy Compliance	↻ C10	An Information and Data privacy compliance plan is in place	○	●	●	●	○
		↻ C11	Agreed actions are closed out	○	●	●	●	○

## 4.2 Key processes and controls

### Process

A set of related activities that must be carried out to achieve policy outcomes

### Controls

The action we put in place to mitigate a risk(s) within a key process and/or the delivery of policy outcomes. These are mandated and are the minimum that should be implemented regardless of any local difference

### Responsibility

for ensuring controls are in place and operating effectively

Ref	Description	Ref	Description	Group (S55 & S56)	Division (S57)	Business Unit (S58)	Contract (S59 & S60)	All Employees (S61)	
P5	Manage Information/Data	➔	C12	Employees responsible for reporting performance, finance and customer information have data integrity as one of their performance objectives	●	●	●	●	○
		➔	C13	All information is classified in accordance with the Group Security Standard and Information Privacy Classification GSOP	●	●	●	●	○
		➔	C14	All Serco business information is treated as confidential, including information obtained regarding Serco's customers and other business partners	●	●	●	●	○
		➔	C15	Records of written consent from customers are maintained where customer information has been publicly disclosed	●	●	●	●	○

### Process

A set of related activities that must be carried out to achieve policy outcomes

### Controls

The action we put in place to mitigate a risk(s) within a key process and/or the delivery of policy outcomes. These are mandated and are the minimum that should be implemented regardless of any local difference

### Responsibility

for ensuring controls are in place and operating effectively

#### Ref Description

#### Ref Description

Group (S55 & S56)  
Division (S57)  
Business Unit (S58)  
Contract (S59 & S60)  
All Employees (S61)

➡	C16	Sensitive information is clearly marked and protected (by confidentiality agreements, security protocols, encryption etc.) to distinguish it from information that is freely disclosable	●	●	●	●	○
➡	C17	Local controls are in place to verify that any records produced or information provided is accurate	●	●	●	●	○
➡	C18	All internal and external financial, performance and compliance information is verifiably accurate and where this cannot be the case, mitigating actions are implemented	●	●	●	●	○
➡	C19	Where mitigating actions cannot be taken to verify the accuracy of performance and compliance information, this has been escalated to your line manager	●	●	●	●	○

### Process

A set of related activities that must be carried out to achieve policy outcomes

### Controls

The action we put in place to mitigate a risk(s) within a key process and/or the delivery of policy outcomes. These are mandated and are the minimum that should be implemented regardless of any local difference

### Responsibility

for ensuring controls are in place and operating effectively

#### Ref Description

P6 Personal Data Protection

#### Ref Description

➡	C20	Local processes are in place to ensure personal data is not disclosed to any third party outside of Serco unless there is: <ul style="list-style-type: none"> <li>• a contractual requirement to do so;</li> <li>• written consent from our customer;</li> <li>• a legitimate business need; or</li> <li>• a legal obligation to disclose</li> </ul>
➡	C21	Local processes are in place to ensure data subject right requests are handled in accordance with relevant and appropriate Serco procedures
➡	C22	Time limits for responding to data subject rights requests are met
➡	C23	A Data Protection Impact Assessment (DPIA) is carried out where a new project, system, technology solution or way of working (or changes to these) are proposed involving intensive or higher risk processing of personal or sensitive personal data
➡	C24	A 'Privacy by design' approach is used for all projects to promote data protection compliance from the start

Group (S55 & S56)	Division (S57)	Business Unit (S58)	Contract (S59 & S60)	All Employees (S61)
<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>

### Process

A set of related activities that must be carried out to achieve policy outcomes

### Controls

The action we put in place to mitigate a risk(s) within a key process and/or the delivery of policy outcomes. These are mandated and are the minimum that should be implemented regardless of any local difference

### Responsibility

for ensuring controls are in place and operating effectively

**Ref**      **Description**  
 P7      Contract document management

Ref	Description
➡ C25	Contract document management procedures are defined, implemented and communicated
➡ C26	All material documents that govern Serco’s contractual relationships, including signed contract documents and variations are held in a safe and secure manner and in accordance with data retention requirements
➡ C27	Where contractual documentation is stored electronically it is securely stored on a Serco managed network with adequate security controls (as required by the security classification)
➡ C28	Where documents are stored on a customer network, and there is no secondary store in a Serco managed network, a document register is maintained, stating document location and access methods, to ensure information is accessible by Serco employees

Group (S55 & S56)	Division (S57)	Business Unit (S58)	Contract (S59 & S60)	All Employees (S61)
●	●	●	●	○
●	●	●	●	○
●	●	●	●	○
●	●	●	●	○



### Process

A set of related activities that must be carried out to achieve policy outcomes

### Controls

The action we put in place to mitigate a risk(s) within a key process and/or the delivery of policy outcomes. These are mandated and are the minimum that should be implemented regardless of any local difference

### Responsibility

for ensuring controls are in place and operating effectively

#### Ref Description

#### Ref Description

Group (S55 & S56)  
Division (S57)  
Business Unit (S58)  
Contract (S59 & S60)  
All Employees (S61)

Ref	Description	Ref	Description	Group (S55 & S56)	Division (S57)	Business Unit (S58)	Contract (S59 & S60)	All Employees (S61)
		↻ C29	Where contractual documentation must be retained in hard-copy format, this is stored in appropriately secured file storage location on Serco premises, on a contract site or at an approved 3rd party archive location	●	●	●	●	○
		↻ C30	Hard copy documents are recorded in a document register that is stored within the contract's electronic document management system	●	●	●	●	○
		↻ C31	A clear audit trail of contractual documents and their changes is maintained to preserve commercial and contractual integrity during the lifetime of service delivery and beyond. All documents are clearly marked with a version number and provide a change history	●	●	●	●	○
P7	Incident Reporting – personal data breach	↻ C32	All personal data breaches are captured, categorised and reported in accordance with defined procedures and all breaches or suspected breaches are immediately reported to the data controller	●	●	●	●	○

### Process

A set of related activities that must be carried out to achieve policy outcomes

### Controls

The action we put in place to mitigate a risk(s) within a key process and/or the delivery of policy outcomes. These are mandated and are the minimum that should be implemented regardless of any local difference

### Responsibility

for ensuring controls are in place and operating effectively

Ref	Description	Ref	Description	Responsibility				
				Group (S55 & S56)	Division (S57)	Business Unit (S58)	Contract (S59 & S60)	All Employees (S61)
		↻ C33	All personal data breaches are recorded on ASSURE and reported to any other appropriate national or other regulatory body in accordance with legal requirements	●	●	●	●	○
		↻ C34	Corrective and preventive actions arising from incident are implemented and communicated	●	●	●	●	○
P8	Freedom of Information	↻ C35	Where there is a statutory or regulatory requirement to do so, processes are in place to ensure compliance in regard to handling requests for information by the public	●	●	●	●	○
P9	Document and Record Management	↻ C36	All data, documents and records are controlled, handled, stored, reviewed and disposed of, appropriate to their security classification, document type and retention period	●	●	●	●	○
		↻ C37	Data retention systems and procedures are established which address the manner in which the particular organisation and employees deal with documents in the various jurisdictions they operate within	●	●	●	●	○

### Process

A set of related activities that must be carried out to achieve policy outcomes

### Controls

The action we put in place to mitigate a risk(s) within a key process and/or the delivery of policy outcomes. These are mandated and are the minimum that should be implemented regardless of any local difference

### Responsibility

for ensuring controls are in place and operating effectively

#### Ref Description

#### Ref Description

Group (S55 & S56)  
 Division (S57)  
 Business Unit (S58)  
 Contract (S59 & S60)  
 All Employees (S61)

➔	C38	Except for any customer-specific document management/retention requirements, all documents and records are managed in accordance with Data Retention and Information Privacy Classification procedures	●	●	●	●	○
➔	C39	Document ownership is clearly defined where operating procedures or supporting documentation are shared with the customer	●	●	●	●	○

## 5 Supporting documentation and guidance

The following should be read in conjunction with this standard:

Ref	Document
SMS-PS-Pr	Privacy Group Policy Statement
SMS-PS-S	Security Group Policy Statement
SMS-PS-II	Information Integrity Group Policy Statement
SMS-PS-P	People Group Policy Statement
SMS-GS-PSC	Procurement and Supply Chain Group Standard
SMS-GS-G1	Consequence Management Group Standard
SMS-GS-BC1	Acceptable Use of Information Systems Group Standard
SMS-GS-S1	Security Group Standard
SMS-GS-F1	Finance Group Standard
SMS-GSOP-S-SECMAN	Security Manual
SMS-GSOP-III1-3	Data Protection Impact Assessments GSOP

## 6 Definitions

Term	Definition
<b>Accountability</b>	Being accountable means being not only responsible for something but also answerable for your actions.
<b>Responsibility</b>	<p>A responsible person is the individual who completes the task required. Responsibility can be shared and delegated.</p> <p>All responsible persons will also be accountable for completing tasks effectively. Non-compliance will have consequences which may include disciplinary action as defined within the Consequence Management Group Standard.</p>
<b>Group</b>	Serco Group plc is the administrative centre of the organisation, responsible for setting corporate strategy, defining governance requirements and supporting the business in its day to day operations
<b>Division</b>	The Group will define a set of business divisions which will be responsible for business delivery within a defined set of markets or geographies.
<b>Business Unit</b>	<p>A Business Unit is a cluster of contracts which provide a similar service e.g. Health, Defence, Transport etc.</p> <p>Where appropriate, a separate legal entity wholly owned or where Serco has a controlling share may also be referred to as a Business Unit, where appropriate.</p> <p>This may also refer to Counties/Territories</p>

Term	Definition
<b>Contract</b>	<p>A Contract provides specified requirements to a customer (either directly with Serco or to a consortium/Joint Venture in which Serco is a party)</p> <p>A Contract will also refer to a corporate/functional area.</p> <p>Corporate/functional areas are functions which support the business and they include finance, HR, procurement etc.</p>
<b>Organisation</b>	Organisation refers to a site, Contract, Business Unit and Division.
<b>Contract Manager</b>	This refers to a manager with responsibility for managing the performance of a contract and can include a Contract Manager on a day-to-day basis (or Operational Manager with devolved responsibility), a Contract Director, Partnership Director and/or a Business Unit Managing Director
<b>Data Handler</b>	A <b>data-handler</b> is any employee who collates, inputs or processes data
<b>Data Owner</b>	A <b>data-owner</b> is the person who is accountable for the integrity and handling of the data, and will often be the Contract Manager
<b>'Natural Persons'</b>	A <b>natural person</b> is a living individual/human being as opposed to a legal entity or organisation

## 7 Further information and support

If you require any further information or support regarding this Group Standard, or if you have any suggestions for improvement, please contact the Accountable Policy Owner (Group) or email [sms@serco.com](mailto:sms@serco.com)