Group Standard Operating Procedure
Data Protection

Document Details

Document Reference	**SMS-GSOP-S1-3**
Version	**4.0**
Issue Date	**June 2020**
Review Date	**June 2022**
Applicability	**Serco Group covering all business regions, operating companies and business units throughout the world**[1]
Authority	**Chief Executive, Serco Group plc**
GSOP Owner	Head of Regulatory, Ethics & Compliance

[1] As used herein, Serco Group and its affiliates, subsidiaries and operating companies are referred to as "Serco", "The Company" or "company", or "we", "us" or "our"

Version history

Version	Date	Reason for release/version update	Issued by
3.0	December 2017	GSOP reviewed and updated in light of GDPR Regulation requirements	Director, Global IT Risk & Assurance
4.0	June 2020	GSOP reviewed - ownership updated, relevant SMS links updated, and privacy replaced with data protection, as needed	Head of Regulatory, Ethics & Compliance

Contents

1 Introduction

This Group Standard Operating Procedure (GSOP) provides a framework for the implementation of data protection management throughout Serco. It sets out the detailed requirements and minimum levels of achievement necessary to implement the data protection elements of the Serco Management System (SMS).

Data protection elements of the SMS are designed to protect information, in particular personal data, which is important to Serco, its employees, customers, suppliers and any other individuals. They also help us to comply with applicable data protection legislation and regulations, such as the EU General Data Protection Regulation 2016/679 (GDPR).

2 Scope

The global nature of Serco's business means that Serco must comply with data protection laws and regulations not only in countries where we have an office, but in all countries to which we market, and from where we collect personal data. This GSOP is designed to ensure compliance with applicable data protection laws, i.e. including the GDPR, and as such should ensure compliance in the majority of the jurisdictions in which we operate.

Serco recognises that although the GDPR has direct effect across all European member states, those member states are permitted to derogate from, and supplement, the GDPR in certain areas. Serco further recognises that some jurisdictions in which it operates may have their own local data protection laws. This GSOP will apply to the maximum extent possible across Serco, except where local requirements contradict with, or are more onerous than those set out in this GSOP, in which case those local requirements will be followed.

3 Objectives and Commitment

The objectives of this GSOP are to set out the requirements and minimum levels of achievement necessary to implement the data protection elements of the SMS and provide further details on the application of the Group Privacy Policy[2], setting out what is required from all Serco employees at all times when processing personal data.

This GSOP is key to Serco's compliance with the data protection requirements set out in the Group Privacy Policy, and its application is mandatory, within the limitations described above.

In order to achieve the above-mentioned objectives and promote good conduct throughout Serco in relation to the processing of personal data, this GSOP sets out data protection principles, as well as overarching data protection requirements.

4 Data Protection Principles and Requirements

4.1 Data Protection Principles

The following data protection principles must be complied with, which apply to the processing of all personal data:

[2] See Group Privacy Policy Ref: SMS-PS-Pr

- personal data must be processed in a fair, lawful and transparent manner
- personal data must be obtained only for one (or more) specific, explicit and legitimate purpose(s) and must not be further processed in any manner incompatible with that/those purpose(s)
- personal data must be adequate, relevant and not excessive in relation to purpose(s) for which it is processed
- personal data must be accurate and, where necessary, kept up to date and every reasonable step must be taken to ensure that personal data that is inaccurate (having regard to the purpose(s) for which it is processed) is immediately deleted or rectified;
- personal data processed for any purpose(s) must not be kept longer than necessary to meet that/those purpose(s)
- appropriate technical and organisational measures must be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data

Personal data will at all times be processed in a manner that can demonstrate compliance with the above-mentioned data protection principles.

4.2 Data Protection Requirements

In addition to the data protection principles set out above, the following overarching requirements set out how personal data should be treated.

- When considering how the data protection principles and overarching requirements apply to the personal data processed, it is important to keep in mind that Serco may act as data controller in certain situations and data processor in others. For example, Serco acts as data processor when it processes the personal data of customers, whereas it acts as data controller when it processes the personal data it collects from data subjects, such as employees.

- Where Serco acts as data processor, it acts on the instructions of customers, which means the company is reliant on customers to tell us how personal data should be used/processed. For example, if a customer receives a data subject access request from one of its data subjects, it may ask Serco to assist it complying with the request or Serco may be under a contractual obligation to assist them.

4.2.1 Rights of Data Subjects

Personal data must be processed in accordance with the rights of data subjects. Data subjects generally have the ability to have access to their personal data upon request and may also be entitled to a number of other rights including:

- the right to rectification of inaccurate personal data
- the right to erasure/delete personal data, commonly referred to as the "right to be forgotten"
- the right to restrict processing under certain circumstances
- the right to data portability
- the right to object (i.e. where personal data are processed for direct marketing purposes) and automated individual decision-making

Customers may ask, or Serco may be under a contractual obligation, to assist customers them to comply with data subject rights requests received from their data subjects. In such situations, it is important that Serco acts on the instructions of customers.

Where Serco receives a data subject right request from one of its data subjects, such as an employee, such a request should be handled in accordance with appropriate Serco policy. For example, if an employee or other persons request access to his/her personal data held by Serco, the request should be handled in accordance with Divisional/local Subject Access Request Procedures. Time limits for responding to data subject rights requests are short, therefore it is important to refer to the relevant procedure as soon as possible following receipt of such a request.

Local Data Protection Champions or Data Protection Officers should be contacted with any queries regarding data subject rights requests received.

4.2.2 Privacy Notices and Fair Processing

Data subjects must be informed about:

- How their personal data is used, including about the types of data collected,
- The purposes for which the data are collected,
- Any third party to whom their personal data may be disclosed and
- The rights available to them
- Any changes to the manner in which their data is processed

In addition, the way in which personal data is held and used must be kept consistent with the privacy notice provided to the data subject. Personal data should be used only as anticipated in the original privacy notice. No further or alternative use should be made of the personal data without first considering the need to obtain 'Informed Consent' from the data subject and/or issuing an updated privacy notice.

It is the responsibility of Serco customers to ensure that their data subjects are informed about how their personal data will be used and that actual usage is in line with their privacy notice.

Further, where Serco acts as data controller, all processing of personal data must be justified by reference to one of a number of 'conditions' for processing. However, in the majority of cases, processing will be justified on the basis that:

- it is in Serco's legitimate interests as a supplier of outsourcing services or an employer, except where such interests are overridden by the interests or fundamental rights and freedoms of data subjects;
- Serco has obtained the data subject's consent (not normally appropriate for employees);
- it is necessary to perform a contracted requirement; or
- it is necessary to comply with a legal obligation

Sensitive personal data should only be processed where it is absolutely necessary to do so. Additional consideration should be given to the secure storage and transmission of sensitive personal data, and access rights should be strictly limited. One of the following conditions must be satisfied in order to process sensitive personal data:

- the explicit consent of the data subject has been obtained, except where consent is precluded under applicable laws;
- the processing is necessary for an obligation of Serco under employment law;
- the vital interests of the data subject need to be protected (e.g. in a medical emergency or other life or death situation); or
- the processing is necessary for the purpose of legal proceedings or obtaining legal advice

If Serco is considering implementing a new project, system, technology or way of working, or making changes to an existing project or way of working, which will involve the processing of personal data, it is important to consider (and record) the condition which can be relied upon together with the rationale for the processing.

In addition, in such situations, consideration should be given to whether a data protection impact assessment should be carried out. Please refer to Serco's Data Protection Impact Assessment GSOP[3] for further details of data protection impact assessments and when they should be carried out.

4.3 Accuracy and Retention

[3] See Data Protection Impact Assessment Ref: SMS-GSOP-II1-3

Personal data must be kept accurate, complete and as up-to-date as practically possible and not retained for longer than the purposes for which it was collected unless there is a clear overriding business need or legal/ regulatory requirement to retain the personal data.

Serco's Data Retention GSOP[4] sets out the procedures for ensuring that data/documents/records are updated, archived and deleted appropriately as well as suggested timeframes for the retention of key categories of data/documents/records.

It is important to note that Serco retains data, documents and records on behalf of its customers (which may contain personal data) and, in such cases, the company may be under customer-specific requirements in respect of the management/retention/disposal of such documentation.

4.3.1 Security of Personal Data

Appropriate technical and organisational security measures must be taken to having proper security for the personal information held. Access and use of personal data must be limited on a strict 'need to know' basis.

Employees should be aware of the obligations within and recommendations set out in the Group Security Standard[5]. Customers may require us to comply with additional security requirements regarding the personal data processed on their behalf. For example, a security questionnaire may be requested to be completed or an audit of security, technical and organisational measures may be undertaken.

4.3.2 Data Protection Impact Assessments (DPIAs)

A Data Protection Impact Assessment must be undertaken before launching any new project, system, technology or way of working (or making changes to an existing project or way of working) which uses significant quantities of personal data, processes sensitive personal data, or processes personal data in novel or high risk ways. Examples of when a DPIA may be required are provided below:

- a new IT system for storing and accessing personal data
- the migration of an existing system holding large volumes of personal data into the cloud
- the conducting of an employee investigation involving the monitoring of employee communications
- using existing personal data for new and unexpected, or more intrusive, purposes
- new Bids
- Mergers and Acquisitions
- new surveillance system (especially one which monitors members of the public)

The Data Protection Impact Assessment (DPIA) GSOP should be referred to in these instances[6]

4.3.3 Data Protection by Design

Data Protection by design is an approach to projects that promotes data protection compliance from the start. This approach should be used in the early stages of any project and then throughout its lifecycle, such as when building new IT systems for storing or accessing personal data, developing legislation, policy or strategies that have data protection implications embarking on a data sharing initiative or using data for new purposes. It is a fundamental component in the design and maintenance of information systems and mode of operation for Serco.

When implementing data protection by design, Serco as data controller needs to take into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the likelihood and severity of risks to the rights and freedoms of natural persons posed by the processing of their personal data.

Serco, by adopting a data protection by design approach, will minimise data protection risks and help build trust. Designing projects, processes, products or systems with data protection in mind at the outset will help

[4] See Data Retention GSOP Ref: SMS-GSOP-II1-2
[5] See Security Group Standard Ref: SMS-GS-S1
[6] See Data Protection Impact Assessment GSOP Ref: SMS-GSOP-II1-3

to ensure core data protection considerations are incorporated into existing project management and risk management methodologies and policies.

4.3.4 Personal Data Breaches

All breaches of personal data should be contained and remedied as soon as possible and, where necessary, all appropriate stakeholders informed of the personal data breach. All employees have an obligation to report data breaches (or suspected data breaches) in accordance with the Incident Reporting and Management GSOP[7] which sets out how personal data breaches should be managed and resolved.

4.3.5 Sharing Data outside of Serco

Personal data should only be disclosed outside Serco where there is a legitimate business need, an overarching legal justification to do this or where a customer consents to such disclosure (whether as set out within a contract or otherwise in writing). Disclosure must be made on a strictly limited 'need to know' basis where there is clear justification for transferring personal data - either because the data subject has consented to the transfer or because it is for a legitimate business need.
Where personal data is transmitted outside Serco, for example to a service provider, a secure medium must be used to transmit such data and written agreements (containing the required level of security standards) should be in place with each such third party.

In each case, data subjects must be aware that the transfer or disclosure is likely to take place to a third party. This should normally be achieved through the use of our End User Privacy Notice or Employee Privacy Notice (or other forms of privacy notice), except where the transfer or disclosure is clearly understood by the data subject as a necessary part of a function of Serco. Assurances should also be sought from the third party recipient that they will only use the personal data for legitimate / authorised purposes and keep it secure.

If a particular disclosure is required to meet a legal obligation (for example to a government agency or police force/security service) or in connection with legal proceedings, the personal data may be provided so long as the disclosure is limited to that which is legally required.

The Procurement Toolkit on Our World should be referred to or local procurement teams where transfers/disclosure of personal data are proposed to be made to third parties.

4.3.6 Transferring Personal Data Overseas

Particular care must be taken when personal data is transferred to a country or territory other than the country where either:

(a) The data subject from which it was collected is resident; or
(b) The Serco entity that collected it is established

Generally, Personal Data originating in the European Economic Area (EEA) must not be transferred outside of the EEA, unless there is a mechanism for ensuring adequate levels of protection for the rights and freedoms of data subjects in relation to the processing of personal data. However, where Serco acts as data processor for customers, transferring personal data outside of the United Kingdom is often restricted, due to customer requirements.

Be aware that transfers may take place that are not obvious. For example, if a supplier of Serco sub-contracts some of its processing obligations to a third party outsource provider in India there will be a transfer of personal data out of the EEA (i.e. from the supplier (who is a data processor of Serco) to the third party outsource provider (who is a sub-processor) which will be prohibited unless certain conditions are met).

Managing overseas data transfers in accordance with these principles requires particular care. Where any personal data is either proposed to be transferred to another country or outside of the EEA or is already being transferred to another country or outside of the EEA, the Data Protection Officer, local Data Protection

[7] Incident & Fraud Reporting and Management GSOP Ref: SMS-GSOP-O1-2

Champions or the Legal team should be contacted who will advise on how to comply applicable data transfer restrictions.

4.3.7 CCTV and Employee Monitoring

CCTV systems should be operated with care to avoid disproportionate risk of privacy intrusion to individual data subjects. CCTV systems should been installed and operated in a way that is proportionate to the risks being covered and prominent notices should be displayed in the area covered by the CCTV system to make sure people are aware that the system is in operation.

Where Serco undertake monitoring on behalf of customers, this will be done in accordance with customer instructions. Where Serco undertakes monitoring on our own behalf, for example, monitoring of employees, any such monitoring should only take place once the relevant employees have been made aware of how and when the monitoring will take place and the possible implications of the monitoring, as well as in accordance with our Acceptable Use of Information Systems Group Standard[8].

Covert monitoring should be avoided other than in exceptional circumstances and only with the prior approval of the Chief Information Officer.

If you have any queries about the use and implementation of CCTV system, please refer to local operating procedures in existence.

5 Consequences of Non-Compliance and Accountability

If Serco is found to be in breach of applicable privacy and data protection laws, the company could face fines and enforcement action from data protection supervisory authorities. Enforcement action will usually have a cost and time implication for the business, as well as the more damaging effect of any restrictions imposed. Additionally, the associated publicity could make Serco appear as an organisation that does not respect the data protection rights of individuals and cause us reputational damage.

It is the responsibility of all our employees to assist Serco to comply with the Group Privacy Policy[9] and this GSOP and ensure processes are in place and followed to handle, manage and process personal data, in accordance with this procedure.

[8] Acceptable Use of Information Systems Group Standard Ref: SMS-GS-BC1

[9] Privacy Group Policy Statement Ref: SMS-PS-Pr

6 Definitions

The following terms are used throughout this GSOP and have particular meanings based on GDPR:

Term Used	Definition
Data Controller	This is a person or company who, either alone or jointly with others, determines the purpose for which, and the manner in which, personal data is processed.
Data Processor	The entity that processes data on behalf of the Data Controller
Data Subject	This is the identified or identifiable living individual whose personal data is being processed. In general, Serco's data subjects include customers, job applicants, employees, suppliers, service providers and business contacts. However, there may be others, including (for example) anyone named on an email sent or received by a Serco Employee.
Employees	This includes all employees (both permanent and temporary), contractors and consultants of Serco
Informed Consent	This means any freely given specific and informed indication of the data subject's agreement to the processing of his/her personal data.
Personal Data	This means any information capable of identifying a living individual, directly or indirectly, in particular by reference a name, identification number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity. The key point is not just to consider the information itself, but the information plus any other information which Serco has access to (which may include information held by a third party). For instance, a full name obviously identifies someone on its own. An identification number does not identify someone in isolation, but if Serco holds a schedule which associates each identification number with a particular individual, then it will still be personal data. Further, if we could reasonably ask a third party for that identifying "link", then the information should also be considered personal data. Personal data can take any form (including electronic data, paper documents and disks) - it could include: alphabetic text (i.e. a name, an opinion about someone, a full address) a number (i.e. an employee ID, identification number, telephone number, IP address) images (i.e. CCTV recording, photograph, medical diagram/photograph) audio data (i.e. telephone recording, recording of an HR interview) biometric data (i.e. fingerprint or iris scan data).
Personal Data Breach	This means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. Examples of personal data breaches include: third party attacks on IT infrastructure designed to harvest personal data for criminal purposes; accidental loss or theft of Serco devices (e.g. mobile phones, laptops, USB devices); the passing to third parties or disposal of personal information without appropriate security measures being in place.

Term Used	Definition
Processing	This means any operation (or set of operations) that is performed upon personal data, whether or not by automatic means, including collection, recording, organisation, storage, access, adaptation, alteration, retrieval, consultation, use, disclosure, dissemination, making available, alignment, combination, blocking, deleting, erasure or destruction (and "**process**", "**processes**" and "**processing**" shall be interpreted accordingly).
Sensitive Personal Data	Certain types of personal data are considered to be 'sensitive' or be 'special categories' of personal data. Additional care needs to be taken when handling such data. Particular care should be taken when collecting and using this type of data (often an individual's explicit consent, or a legal obligation, to do so will be sought). Sensitive personal data means any information relating to: • medical and biometric information • racial or ethnic origin • criminal convictions • political opinions • religious beliefs or political or philosophical opinion • trade union membership • sex life or sexual orientation • genetic data While financial data (such as bank account or credit card details or salary information) are not included in the above-mentioned list of sensitive personal data, this information should be treated as sensitive for obvious reasons.

7 References

The following should be read in conjunction with this GSOP:

Reference	Location	Title
SMS-PS-Pr	SMS>Information Integrity>Policies	Group Privacy Policy
SMS-GS-II1	SMS> Information Integrity>Standards	Information and Data Privacy Group Standard
SMS-GS-S1	SMS>Security>Standards	Security Standard
SMS-GS-BC1	SMS>Business Conduct & Ethics>Standards	Acceptable Use of Information Systems
SMS-GSOP-O1-2	SMS>Operations>Group SOPs	Incident & Fraud Reporting and Management GSOP
SMS-GSOP-II1-3	SMS>Information Integrity>Group SOPs	Data Protection Impact Assessment GSOP
SMS-GSOP-S-SECMAN	SMS>Security>Group SOPs	Security Manual GSOP
SMS-GSOP-II1-2	SMS>Information Integrity>Group SOPs	Data Retention GSOP
N/A	https://serco.sharepoint.com/sites/ProcurementKnowledgeSite/Shared%20Documents/Forms/AllItems.aspx?csf=1&e=eULUdL&cid=2974b01d%2Deac3%2D4e85%2Da22d%2D458c5672bbb9&FolderCTID=0x012000C4B8487E47F8994FB1E99A6EF51A8F41&viewid=b91447e6%2Ddb4d%2D4eeb%2D82a9%2D9e3384ad5b77	Procurement Toolkit

Supporting policy and guidance documentation relating to the Serco Group IT Policies and Controls is available in the IT Governance and Compliance area of the Information Management and Technology site that can be accessed on MySerco and on the Serco Intranet/SharePoint.