Policy Document

OCS Group Limited – Data Protection Policy

January2021 / v4.0

1.0 Policy Objectives

The purpose of this Policy is:

1. to outline the responsibilities of those within the organisation who are handling Data including Personal Data as part of their role

2. to set out the requirements of good practice guidelines when handling Personal Data

3. to set a standard of compliance with data protection laws

2.0 Policy Scope

Personal Data is 'any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identify of that natural person'. Different pieces of information, which collected together can lead to the identification of a particular person, also constitute personal data.

Special Category Data previously known as 'sensitive data' refers to Personal Data which requires additional protection due to the sensitivity of the content such as data regarding race or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, health data, biometric data, data concerning a person's sex life or data concerning a person's sexual orientation.

This policy applies to all Personal Data and Special Category Data acquired, received, processed, stored, amended, disclosed and erased by OCS in the conduct of its business as usual activities, in electronic format in any medium and within structured paper filing systems. This shall include OCS data, as well as personal data owned by an external organisation, and entrusted to OCS under a contract which specifically communicates data protection requirements.

This Data Protection Policy applies to all OCS employees, whether permanent, temporary, contractors or consultants; third party users; external Data Processors, and any other organisation or individual with a bona-fide need to process Personal Data held by OCS.

Disciplinary action may be taken against staff failing to comply with this policy. Failure to comply with data protection legislation may result in legal action being taken against the individual and/or the organisation.

The Data Protection team should be contacted at DataProtection@ocs.com in relation to any queries arising regarding data protection and privacy matters.

3.0 Policy Statements

Data protection legislation sets out the rules for how OCS must process Personal Data and Special Category Data about living individuals. OCS is committed to protecting personal information from loss, misuse, disclosure, alteration, unavailability, unauthorised access and destruction and takes all reasonable precautions to safeguard the confidentiality of personal information, including through use of appropriate organisational and technical measures.

OCS needs to collect and process Personal Data about people, including staff and individuals with whom it deals with, in order to operate its daily business. OCS must have a lawful purpose for holding and processing the data. As part of its compliance commitments, OCS shall implement appropriate measures to ensure that personal information is:

- processed lawfully, fairly and in a transparent manner.
- collected for specific, explicit and legitimate (stated) purposes under a documented lawful basis and not further processed in a manner that is incompatible with those purposes as outlined in the organisation's **Record of Processing Activities (RoPA)**
- adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed as documented in the **Data Protection Impact Assessment (DPIA)** as appropriate
- accurate and, where necessary, kept up to date – any inaccuracies must be fixed or removed without undue delay.
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the Personal Data is processed in accordance with the Data Retention Policy.
- Personal Data shall only be processed subject to implementation of the appropriate technical and organisational measures required by the applicable privacy and data protection legislation in order to safeguard the rights and freedoms of the data subject.
- 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 as outlined in the Information Security Policy framework.

OCS is committed to ensuring that staff are appropriately trained and supported to achieve and maintain data protection compliance.

4.0 Policy Principles

4.1 Lawful, Fair and Transparent Data Processing

Please refer to Guidance Note OCSIS-G-007 for further information on Privacy Statements & Transparency, OCSIS-G-011 for General Records Management Considerations and OCSIS-G-004 for Data Privacy by Design and Default

- There shall be an established lawful basis for processing for all Personal Data sets processed by OCS by the information asset owner, outlined in the RoPA and agreed with the **Data Protection Officer (DPO),** as applicable.
- Where Special Category Data is to be processed, there shall be an additional lawful basis for the processing as required by the legislation and agreed by the DPO, as applicable.
- There shall be centralised privacy notices in place to outline business as usual processing practices conducted on Personal Data.
- All staff, including where appropriate contractors and key integrated third party functions, as agreed by the DPO, shall complete the mandatory data protection training upon starting employment with OCS.
- All Personal Data shall be handled in accordance with the **Data Retention Policy OCSIS-P-11**.
- A privacy statement shall be presented to data subjects when personal data is collected from them in accordance with the circumstances within which their data was obtained, be this directly from the individual or from a third party.

4.2 Data Minimisation

Please refer to Guidance Note OCSIS-G-032 for further information on Data Collection and OCSIS-G-031 for Data Processing and OCSIS-G-004 for Data Privacy by Design and Default

- The organisation shall hold no more Personal Data than is strictly necessary for the performance of its specific obligations
- The principle of 'data privacy by design and default' shall be fulfilled by the completion of DPIAs where necessary, to determine the Personal Data required to fulfil the purpose
- Any Personal Data collected via electronic means or on paper, shall be scrutinised to ensure that only the required personal data sets are included and no excessive processing is being conducted.
- The organisation shall regularly review and monitor its data collection mechanisms and practices to ensure compliance with the data minimisation principle
- OCS shall only share Personal Data where it is necessary for the agreed purpose
- No Personal Data shall be shared without explicit justification as to why it is required by the recipient
- Data shall be held in strict accordance with the Records Retention Policy and Records Retention Schedule.

4.3 Governance of Data Protection Policy and Data Protection Officer

- Data protection compliance is everyone's responsibility and individuals will be held to account where they fail to implement good information management practices.

- Data protection and privacy risk shall be assessed and owned by the relevant information asset owner as appropriate, or business function conducting the processing of Personal Data.

- OCS shall have a DPO who shall monitor the internal compliance posture, inform and advise the business on its data protection obligations, provide advice around DPIAs and act as a contact point for data subjects and the supervisory authority. of data protection matters within the organisation.

- The DPO shall be supported by a data protection team who shall be the contact point for business as usual queries regarding data protection and privacy compliance.

- Senior management fully endorse the contents of this Policy and reserve the right to take action where they believe an individual has failed to meet their obligations under such.

4.4 Responsibilities

4.4.1 Data Protection Officer (DPO)

The DPO is responsible for:

- advising OCS and its staff of obligations under data protection legislation
- monitoring compliance with relevant data protection laws and regulations, business policies relating to data protection and privacy, monitoring training and audit activities relating to data protection compliance
- providing advice as necessary on the completion and highlighted risks on DPIAs
- co-operating with and acting as the contact point for supervisory authorities
- having due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

4.4.2 Staff Responsibilities

OCS staff who process Personal Data about job applicants, colleagues, suppliers, clients or any other individual must comply with the requirements of this policy. Staff members must ensure that:

- they complete their data protection and information security training modules as requested;
- all Personal Data is kept securely;
- no Personal Data is disclosed either verbally or in writing, accidentally or otherwise, to any unauthorised third party; where there is any doubt, contact the data protection team or DPO for advice;
- Personal Data is kept in accordance with the records retention schedule;
- any queries regarding data protection, including data subject rights requests and complaints, are promptly directed to the data protection team at dataprotection@ocs.com ;
- any data protection breaches are brought to the attention of the data protection team immediately and the DPO and that they support the data protection team in resolving breaches;

4.4.3 Contractors, Short Term or Voluntary Staff Responsibilities

Managers who employ contractors, short term or voluntary staff must ensure:

- individuals are appropriately vetted for the data they will be processing.
- any Personal Data collected or processed in the course of work undertaken for OCS is kept securely and confidentially at all times;
- all Personal Data is returned to OCS on completion of the work or securely destroyed, including any copies or back-ups that may have been made.
- any Personal Data made available by OCS is neither stored nor processed outside the UK or shared with another party, unless written consent to do so has been received from OCS
- all practical and reasonable steps are taken to ensure that contractors, short term or voluntary staff do not have access to any Personal Data beyond what is essential for the work to be carried out properly.

4.4.3 Third Party Data Processors

Where external companies are used to process Personal Data on behalf of OCS, responsibility for the security and appropriate use of that data remains with OCS. Where a third-party data processor is used:

- a company must be chosen which provides sufficient guarantees about its security measures to protect the processing of Personal Data;
- the information security team should be consulted to assess whether sufficient security measures are in place;
- a written contract in the form of a Data Processing Agreement, establishing what Personal Data will be processed, for what purpose and the obligations on both OCS and the other company, must be signed by both parties.

4.5 Review of Data Processing Practices

Please refer to Guidance Note OCSIS-G-004 for further information on Data Privacy by Design and Default

- There shall be a DPIA completed at the outset of writing a business case for a new system or implementing a new process.
- All DPIA documents shall be sent to the data protection team for review and sign off before a project or purchase commences.
- A review of the RoPA shall be completed annually, to ensure that all new processes are accounted for and changes documented.
- The data protection team should be consulted in relation to any queries arising regarding data protection and privacy matters.

4.6 Data Sharing – Disclosure of Personal Information

Please refer to Guidance Note OCSIS-G-013 for further information on Data Sharing and Guidance Note OCSIS-G-035 for Anonymisation and Pseudonymisation

- Data sharing can take any of the following formats:
    1. Data exchange between two or more parties
    2. One organisation sending data to another
    3. Several organisations collaborating data and making this available to all involved organisations or a third party
    4. One-off disclosures of information
    5. Sending data internally between colleagues or departments.
- Personal Data in any format will not be shared with a third-party organisation without a valid business reason.
- A signed Data Processing Agreement (DPA) or a Data Sharing Agreement [DSA] should be in place where data is being sent to an external party.
- The DPA/DSA drafting process will be overseen by the data protection and legal teams to ensure that all OCS security requirements are addressed in the contract.
- Where data is being shared internally, it should be limited to only that required to fulfil the purpose on a 'need-to-know' basis.
- The confidential nature of the data shall be considered prior to any form of sharing both internally and externally
- All data sharing shall be via secure means to mitigate the risk to the data during transit
- Where possible, data shall be anonymised or pseudonymised prior to any sharing internally or externally
- Where there is to be an international transfer of Personal Data, the data protection and legal teams must be consulted.

4.7 Data Subject Rights

Please refer to Guidance Note OCSIS-G-009 for further information on Data Subject Rights

- All data subject rights requests shall be handled in accordance with internal OCS procedures and the relevant data protection legislation.
- All requests shall be notified to the data protection team as soon as possible upon receipt and no later than one business day after receipt.
- All individuals will fully co-operate with requests from the Data Protection team to assist with the handling of a data subject right request.

4.8 Marketing and ePrivacy Considerations

Please refer to Guidance Note OCSIS-G-008 for further information on B2B Comms and Direct Marketing

- There shall be no direct marketing to individuals without their recorded specific consent being held by OCS in line with internal procedures for collecting, storing and maintaining records of consent.
- Where an individual 'opts-out' of receiving further marketing communications, they will be added to a 'do not contact' list held and maintained by External Communications, for audit purposes, to prevent future correspondence from being sent.

4.9 Systems Security – Technical & Organisational Measures

- OCS shall ensure that all new systems and applications are reviewed and assessed by the Information Security team.
- The DPIA document will account for the technical and organisational measures to be put in place to facilitate the processing.
- All staff members shall abide by the IT Security Policy at all times.
- All third party system providers shall enter into contractual arrangements with OCS, outlining the parties respective obligations around security and the processing of Personal Data.

4.10 Data Breach/Loss Notification

Please refer to Guidance Note OCSIS-G-006 for further information on Data Breaches

- Staff will report any actual or suspected data breaches to the DPO for investigation by emailing DataProtection@ocs.com immediately upon becoming aware of the breach, outlining the details required to conduct a review, in accordance with Guidance Note OCSIS-G-006 Data Breaches.
- Staff will promptly assist the data breach investigation team with any enquiries and investigations they may instigate as a result of the breach.

5.0 Policy Communication

This policy will be made available:

- internally to all staff by being declared as a record and stored within the appropriate Office Policies Site on the Intranet.
- externally by publishing it on the OCS website.

Further Questions or Making a Complaint

If you have any queries or complaints about our collection, use or storage of your personal information, or if you wish to exercise any of your rights in relation to your personal information, please contact our Data Protection Officer - email dataprotection@ocs.com or write to Data Protection Officer, OCS Group Limited, 4 Tilgate Forest Business Park, Brighton Road, Crawley, RH11 9BP. We will investigate and attempt to resolve any such complaint or dispute regarding the use or disclosure of your personal information. You may also make a complaint to the Information Commissioner's Office (ICO) on 0303 123 1113 or by writing to Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.

6.0 Policy Exceptions

None

7.0 Policy Awareness

All OCS employees, contractors, and agents are expected to adhere to the provisions of this policy. Managers and supervisors are expected to promote awareness of this policy and ensure it is adhered to by all staff. This policy applies to all staff, and will be communicated to OCS suppliers, contractors, business affiliates and wider stakeholders as necessary. All personnel should be aware that a failure to comply with this policy, including any arrangements which are put in place under it, will be investigated and may lead to disciplinary action being taken, up to and including termination of employment. In cases where the failure to comply has resulted in a breach of legislation the individual and OCS may be vulnerable to prosecution. The objectives shall be signed off by senior management, tracked by the ISMS owner and reviewed annually with management.

8.0 Document Control

This Policy will be formally reviewed on an annual basis, as a minimum, or if required changes are identified to address one or more of the following:

- A change in business activities, which will or could possibly affect the current operation of OCS Information Security Management System, and the relevance of this document.
- A change in the way OCS manages or operates its information assets and/or their supporting assets, which may affect the accuracy of this document.
- An identified shortcoming in the effectiveness of this Policy, for example as a result of a reported information security incident, formal review or an audit finding.

The current version of this Policy, together with its previous versions, shall be recorded below.

Version	Description	
1.0	Date Live:	25.04.2017
	Notes/Author:	*David Carvalho, Group CISO*
	Reviewed by:	*David Carvalho, Group CISO*
	Approved by:	Richard Baylie, Group CISO
2.0	Date Live:	06.06.2018
	Notes/Author:	David Coleman
	Reviewed by:	Andrea Simmons
	Approved by:	Richard Baylie, Group CISO
3.0	Date Live:	12.04.2019
	Reviewed by:	Melanie Hyatt-Steel, Technical Compliance Manager
	Approved by:	Richard Baylie, Group CIO
4.0	Date Live:	19.01.2021
	Reviewed by:	Melanie Hyatt-Steel; Technical Compliance and ISMS Manager Samantha Smith; Data Protection and Privacy Manager
	Approved by:	Richard Baylie; Group CIO