Data Protection Policy - Global

OCSIS-P-10

TRUE.Values.

1. About this policy

1.1 Everyone has rights with regard to the way in which their personal data is handled. During the course of our activities we will collect, store and process personal data about our colleagues, clients, customers and suppliers. OCS Group Holdings Ltd and all it's subsidiaries (OCS) take our data protection responsibilities extremely seriously and recognise that the correct and lawful treatment of this data will maintain confidence in the organisation and will provide for successful business operations.

1.2 All colleagues are obliged to comply with this policy when processing personal data on our behalf and any breach of this policy may result in disciplinary action.

1.3 The types of personal data that we process include information about current, past and prospective suppliers, customers, tenants, landlords, colleagues, professional advisers, consultants and others we may communicate with. The personal data we hold is subject to the highest legal standard globally, the EU General Data Protection Regulation 2016 (GDPR). Countries that we operate in will have regional variations and there are country specific policies for that reason.

1.4 This policy and any other documents referred to in it sets out the basis on which we will process any personal data we collect from data subjects or other sources. It also sets out rules on data protection and the legal conditions that must be satisfied when we obtain, handle, process, transfer and store personal data.

2. Who this policy applies to

2.1 This policy applies to all Global colleagues, officers, consultants, contractors, casual workers and agency workers who we employ and work with. This policy does not form part of any colleague's contract of employment and may be amended at any time.

3. Responsibility for this policy

3.1 OCS directors have overall responsibility for the effective operation of this policy but has delegated responsibility for overseeing its implementation to the Data Protection Officer. Suggestions for change should be reported to the Data Protection Officer.

3.2 The data protection team has day-to-day responsibility for this policy, and you should refer any questions about this policy to them in the first instance at dataprotection@ocs.com

3.3 This policy is reviewed annually by the Data Protection Officer.

4. Definition of Data Protection terms

4.1 Data is information, which is stored electronically, on a computer, or in paper-based filing systems.

4.2 Data subjects for the purpose of this policy include all living individuals about whom we hold personal data. All data subjects have legal rights in relation to their personal information.

4.3 Personal data means data relating to a living individual who can be identified directly or indirectly from that data (or from other information in our possession)

4.4 A data controller is the organisation that determines the purposes and means of the processing of personal data. They are responsible for establishing practices and policies in line with legislation. OCS are the data controller of all personal data of our employees.

4.5 Data processors include any person or organisation that processes personal data on behalf of a data controller. This includes suppliers which handle personal data on behalf of OCS or it's subsidiaries.

4.6 Processing is any activity that involves the use of data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

4.7 Special category data includes information about a person's racial or ethnic origin, political opinions, religious beliefs, trade union membership, physical or mental health or sex life or in relation to a criminal offence committed or alleged to have been committed by that person. Special category data can only be processed under specific circumstances.

5. Data Protection Principles

5.1 There are 7 data protection principles that are the foundation of data protection law. Personal data must be:

- Processed fairly, lawfully and transparently;
- Processed for specified, legitimate purposes;
- Adequate, relevant and limited to what is necessary;
- Accurate and kept up to date;
- Not kept longer than necessary for the purpose;
- Kept securely with appropriate technical and organisational measures;
- Accountability - as an organisation we are responsible for complying with the legislation and demonstrating our compliance.

6. Fair and Lawful Processing

6.1 The GDPR is not intended to prevent the processing of personal data but to ensure that it is done fairly and without adversely affecting the rights of the data subject.

6.2 For personal data to be processed lawfully, it must be processed on the basis of one of the legal grounds set out in the Regulation. These include, the data subjects consent, the processing is necessary for the performance of a contract, for the compliance with a legal obligation to which the data controller is subject, or for the legitimate interest of the data controller or the party to who, the data is disclosed. Where special category data is being processed, additional conditions must be met. When processing personal data as data controllers in the course of our business, we will ensure that those requirements are met.

7. Processing for limited Purposes

7.1 In the course of our business, we may collect and process the personal data set out in the schedule to this policy. This may include data we receive directly from a data subject (for example, by completing forms or by corresponding with us by mail, phone, email or otherwise) and data we receive from other sources (including for example business partners, sub-contractors in technical, payment and delivery services, credit reference agencies and others).

7.2 We will only process personal data for the specific purposes set out in the schedule to this policy or for any other purposes specifically permitted by the Regulation. We will notify those purposes to the data subject when we first collect the data or as soon as possible thereafter.

8. Notifying Data Subjects

8.1 If we collect personal data directly from data subjects, we will inform them about:

- The purpose or purposes for which we intend to process that personal data;
- The types of third parties we will share or disclose that personal data to;
- The means with which data subjects can limit our use and disclosure of their personal data.

8.2 If we receive personal data about a data subject from other sources, we will provide the data subject with this information as soon as possible.

8.3 We will also inform data subjects whose personal data we process that we are the data controller with regard to that data.

9. Adequate, Relevant and Limited Processing

9.1 We will only collect personal data to the extent that it is required for the specific purpose notified to the data subject.

10. Accurate Data

10.1 We will ensure that personal data we hold is accurate and kept up to date. We will check the accuracy of any personal data at the point of collection and we will take all reasonable steps to destroy or amend inaccurate or out-of-date data.

11. Timely Processing

11.1 We will not keep personal data longer than is necessary for the purpose or purposes for which it was collected. We will take all reasonable steps to destroy, or erase from our systems, data which is no longer required.

12. Processing in line with Data Subject's Rights

12.1 We will process all personal data in line with data subjects rights, in particular their right to:

- Request access to any data held about them by a data controller (see also clause 16),
- Prevent the processing of their data for direct marketing purposes;
- Ask to have inaccurate data amended (see clause 10)

13. Data Security

13.1 We will take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

13.2 We will put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Each of our colleagues is responsible for protecting the personal data they work with and have access to. They must follow all procedures and technologies in place to maintain the security of personal data.

13.3 To maintain data security by protecting the confidentiality, integrity and availability of the personal data we and each of our colleagues must:

- keep personal data confidential, which means that only people who are authorised to use the data can access it,
- maintain the integrity of personal data, which means that personal data should be accurate and suitable for the purpose for which it is processed,
- protect the availability of personal data. Only authorised users should be able to access data for specified purposes. Personal data should always be saved in agreed folders which are appropriately backed up and not on any personal drive or device.

13.4 Security procedures that our colleagues must follow include:

- Entry controls. Any stranger seen in entry controlled areas should be reported;
- Secure lockable desks and cupboards. Desk and cupboards should be kept locked if they hold confidential information of any kind;
- Disposal. Paper documents should be shredded or placed in confidential waste bins. Further advice from the data protection officer should be sought if none of these options are available. Digital devices should be returned to IT when they are no longer required.
- Monitors. All colleagues must ensure confidential information is not visible to anyone in their work area. All PCs should be locked (CTRL-ALT-DEL) when they are unattended.

14. Transferring Personal Data to a Country Outside the EEA

14.1 We may transfer personal data to a country outside the European Economic Area (EEA) provided that one of the following conditions applies:

- The country to which the personal data is transferred ensures an adequate level of protection for the data subjects rights and freedoms;
- The data subject has given their consent;
- The transfer is necessary for the performance of a contract between us and the data subject;
- The transfer is legally required on public interest grounds or for the establishment, exercise or defence of legal claims.

14.2 Subject to the requirements in clause 13 above personal data we hold may also be processed by colleagues operating outside the EEA who work for us or for one of our suppliers. This work will include the fulfilment of contract with the data subject, the processing of payment details and the provision of support services.

15. Disclosure and Sharing of Personal Information

15.1 We may share personal data we hold with any member of our group i.e. our subsidiaries, our ultimate holding company and its subsidiaries, as defined in section 1159 of the UK Companies Regulation 2006.

15.2 We may also disclose personal data we hold to third parties:

15.2.1 In the event that we sell or buy any business or assets, in which case we may disclose personal data we hold to the prospective seller or buyer of such business or assets,

15.2.2 If we or substantially all of our assets are acquired by a third party, in which case personal data we hold will be one of the transferred assets, or

15.2.3 If we are under a duty to disclose or share a data subject's personal data in order to comply with any legal obligation, or in order to enforce or apply any contract with the data subject or other agreements; or to protect our rights, property, or safety of our colleagues, customers, or others. This includes exchanging information with other companies and organisations for the purposes of fraud protection and credit risk reduction.

15.3 We may also share personal data we hold with selected third parties for the purposes set out in the schedule to this policy.

16. Dealing with Subject Access Requests

16.1 Data subjects can make requests for information we hold about them. The request may be written or verbal. Colleagues who receive a request to disclose information held in connection with a data subject should notify the Data Protection Officer immediately via dataprotection@ocs.com

16.2 The Data Protection Officer will verify the identity of an individual requesting data under any of the rights afforded by the GDPR. Do not allow third parties to persuade you into disclosing personal data without proper authorisation from the Data Protection Officer.

17. Reporting a Personal Data Breach

17.1 We have put in place procedures to deal with suspected loss of or unauthorised access to personal data (a "personal data breach") that are available on our intranet or on request from the Data Protection Officer. Each of our colleagues must comply with these procedures.

17.2 If you know or suspect that a personal data breach has occurred, please do not attempt to investigate the matter yourself. Please contact the Data Protection Officer as quickly as possible at dataprotection@ocs.com

18 Changes to this Policy

18.1 We reserve the right to change this policy at any time. Where appropriate, we will notify data subjects of those changes by mail or email.

Schedule

Data Processing Activities

- Reasons/Purposes for Processing Information

We process personal information to enable us as to carry out property management services; promote and advertise our services; maintain our own accounts and records; and support and manage our colleagues.

- Type/Classes of Information Processed

We process information relevant to the above reasons/purposes. This may include:

- Personal details
- Family details
- Lifestyle and social circumstances
- Employment and education details
- Financial details
- All information contained in references

We may also process special category data that may include:

- racial or ethnic origin
- religious or other beliefs
- trade union membership
- physical or mental health details

Data Subjects include:

- customers
- tenants
- professional advisers and consultants
- complainants, enquirers
- suppliers
- landlords
- colleagues

Document Control

Version	Description	
1.0 New Global Policy	Date live	November 2023
	Reviewed by	Sara Taylor, DPO
	Approved by	
2.0	Date live	January 2025
Annual review – no material changes	Reviewed by	
	Approved by	
	Date live	
	Reviewed by	
	Approved by	