



Issued by / Contact: Group Finance Director

## 1. Background

- 1.1 Organisations that process Personal Data, must comply with the Data Protection Legislation (as defined below), which includes a set of data protection principles that create standards for fair and lawful processing of Personal Data.

Companies within Osborne Group Holdings Ltd ("**Osborne**" or "**we**" or "**our**" or "**us**") process Personal Data relating to clients, tenants, company representatives and our own employees and contractors.

**Definition** of data protection terms:

### "Controller"

means the people who or organisations which, alone or jointly with others, determine the purposes for which, and the means of the processing of Personal Data. They are responsible for establishing practices and policies in line with Data Protection Legislation. We are the data controller of all Personal Data used in our business for our own commercial purposes.

### "Data"

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

### "Data Protection Legislation"

means the Data Protection Act 2018 (the "DPA") and the General Data Protection Regulation 2016/679 (the "GDPR") until any UK data protection legislation replaces the GDPR in the UK.

### "Data Users"

means those of our employees whose work involves processing Personal Data. Data users must protect the data they handle in accordance with this data protection policy and any applicable data security procedures at all times.

### "Data Protection Officer" or "DPO"

means the data protection officer appointed pursuant to the Data Protection Legislation.

### "Personal Data"

means any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a 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 identity of that natural person ("Data Subject"). A Data Subject need not be a UK national or resident. All Data Subjects have legal rights in relation to their Personal Data.

### "People Team"

means the team administering human resources, policies and procedures.

**“Policy”**

means this data protection and privacy policy.

**“Processing”**

means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

**“Processor”**

means any person or organisation that is not a data user that processes Personal Data on our behalf and on our instructions. Employees of data controllers (i.e. our employees) are excluded from this definition but it could include suppliers which handle Personal Data on behalf of Osborne.

**“Special categories of Personal Data”**

means Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. Sensitive Personal Data can only be processed under strict conditions, including a condition requiring the explicit permission of the person concerned.

**2. Policy**

- 2.1 Everyone has rights with regards to the way in which their Personal Data is handled. During the course of our activities we will collect and process Personal Data about our customers, suppliers, our employees and other third parties and we recognise that the correct and lawful treatment of this data will maintain confidence in the organisation and will provide for successful business operations.
- 2.2 All the Data Users are obliged to comply with this Policy when processing Personal Data on our behalf. Any breach of this Policy may result in disciplinary action.
- 2.3 This policy does not form part of any employee's contract of employment and may be amended at any time.
- 2.4 This policy has been approved by Osborne Group Holdings Limited's board of directors. It sets out rules on data protection and the legal conditions that must be satisfied when we obtain, handle, process, transfer and store Personal Data.
- 2.5 The Group Finance Director is responsible for the general administration of this policy throughout the Osborne Group and will be the first point of contact for anyone who has a question or concern about this policy or its application. In order to contact the Group Finance Director on telephone 0800 025 8008 or email [dataprotection@osborne.co.uk](mailto:dataprotection@osborne.co.uk).
- 2.6 The Data Protection Officer (DPO) is responsible for ensuring compliance with Data Protection Legislation and with this Policy. That post is held by Colin Brewer, Business Logistics Director; 0800 025 8008;



dataprotection@osborne.co.uk. Any concerns about a breach of Data Protection Legislation or a concern that the policy has not been followed, should be referred in the first instance to the Group Finance Director or the DPO.

### 3. Objectives

3.1 We handle information including:

- a) Personal Data;
- b) Commercially sensitive information;
- c) Business information; and
- d) Trade secrets and know-how.

3.2 All of these categories are critical to our successful operation. We have decided that it is appropriate to treat all information in our care and control with the same degree of security and confidentiality.

3.3 The objectives of this Data Protection and Privacy Policy are:

- a) To coordinate the information securely and data handling procedures we have in force;
- b) To promote confidence in our Information security and data handling procedures;
- c) To provide assurances for third parties dealing with us;
- d) To comply with the Data Protection Legislation;
- e) To provide a benchmark for employees on information security, confidentiality and data protection issues.

3.4 Everyone should be able to feel reassurance that the information (or Personal Data) held on them by us or by our appointed Processors is relevant, accurate and secure. We are entitled to use Personal Data for administrative and management purposes and to meet legal obligations. We will ensure that it is not misused or passed onto others without permission, unless the law requires, or is for administrative and management purposes, or duty of care to you.

3.5 Where we seek Personal Data from you in connection with your work or application to work for the Osborne group of companies (the "Group"), you will be informed as to why this information is being collected and how it will be used.

3.6 We will aim to ensure that all Personal Data is processed in accordance with Data Protection Legislation. Anyone processing Personal Data must comply with the principles of good practice under Data Protection Legislation. These provide that Personal Data must be:

- a) Obtained and processed fairly, lawfully and in a transparent manner in relation to the Data Subject;
- b) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');



- d) Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that Personal Data that is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay ('accuracy');
- e) Kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data is processed;
- f) Processed in line with the rights of the individual under Data Protection Legislation including the right of the individuals to access Personal Data that relates to them when they reasonably request it;
- g) 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 ('integrity and confidentiality');
- h) Not transferred to countries outside of the European Economic Area (EEA), or to a territory outside the European Economic Area (the "EEA") in respect of which the European Commission has not made a positive finding of adequacy, without adequate protection.

#### 4. Fair and lawful processing

- 4.1 The Data Protection Legislation 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.
- 4.2 We will process the Personal Data of the individuals lawfully, fairly and in a transparent manner in relation to the individuals.
- 4.3 Before any Personal Data may be processed, a legal ground for processing must be met and, when Special Categories of Data are being processed, additional conditions must be met.
- 4.4 The legal grounds for processing that are likely to apply in a commercial context, are where the Data Subject has consented to the processing for one or more specific purposes or where the processing is necessary for the performance of any contract to which the individual is party. Processing is also permitted where it is necessary for the legitimate interests of the Controller or a third party to whom the data is disclosed, except where such interests are overridden by the interests or fundamental rights and freedoms of the individual.
- 4.5 When processing Personal Data as data controllers in the course of our business, we will ensure that those requirements are met.

#### 5. Processing for limited purposes (Purpose Limitation)

- 5.1 Data must be obtained only for specified, explicit and legitimate purposes and not further processed in a manner that is



incompatible with those specified lawful purposes.

5.2 In the course of our business, we may collect and process the Personal Data set out in Schedule 1. This may include Personal 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 Personal Data we receive from other sources (including, for example, business partners, sub-contractors, payment and delivery service suppliers, credit reference agencies and others).

5.3 We will only process Personal Data for the specific purposes set out in Schedule 1 or for any other purposes specifically permitted by Data Protection Legislation. We will notify those purposes to the Data Subject when we first collect the data or as soon as possible thereafter.

5.4 Schedule 1 to the Policy will be kept up-to-date to reflect the organisation's current Processing activities.

## 6. Notifying Data Subjects

6.1 Compliance with the fair processing requirement requires the provision of certain information to individuals, so far as practicable. As a general rule, the Controller must provide the information before it collects the Personal Data. Where the Controller does not obtain the Personal Data directly from the Data Subject, Data Protection Legislation provides that the information may instead be provided as soon as practicable after first Processing;

6.2 If we collect Personal Data directly from Data Subjects, we will inform them about:

- a) The purpose or purposes for which we intend to process that Personal Data.
- b) The types of third parties, if any, with whom we will share or to whom we will disclose that Personal Data.
- c) The means, if any, by which Data Subjects can limit our use and disclosure of their Personal Data.

6.3 If we receive Personal Data about a Data Subject from third parties in our capacity as a Controller, we will inform the Data Subjects that we are the Controller with regard to that Personal data.

## 7. Adequate, relevant and non-excessive processing

7.1 We will only collect Personal Data to the extent that it is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

## 8. Accurate data

8.1 We will keep the Personal Data we process accurate and, where necessary, kept up to date. We will take every reasonable step to ensure the Personal Data that is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay;

## 9. Data retention

9.1 Personal Data must not be kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the Personal Data is processed (for example, where data is collected for a specific marketing



campaign, once the campaign is completed, the data should be deleted).

- 9.2 We will take all reasonable steps to destroy, or erase from our systems, all Personal Data which is no longer required.

## 10. Processing in line with Data Subject's rights

The Data Subjects have the following rights:

### 10.1 Data Subjects access requests:

The relevant Data Subject has the right to obtain from us confirmation as to whether or not Personal Data concerning him or her is being Processed, and, where that is the case, access to the Personal Data and the following information:

- a) the purposes of the Processing;
- b) the categories of Personal Data concerned;
- c) the recipients or categories of recipient to whom the Personal Data have been or will be disclosed, in particular recipients in third countries or international organisations;
- d) where possible, the envisaged period for which the Personal Data will be stored, or, if not possible, the criteria used to determine that period;
- e) the existence of the right to request from the controller rectification or erasure of Personal Data or restriction of processing of Personal Data concerning the Data Subject or to object to such processing;

- f) the right to lodge a complaint with a supervisory authority;
- g) where the Personal Data is not collected from the Data Subject, any available information as to the source;
- h) the existence of automated decision-making, including profiling, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the Data Subject;
- i) Where Personal Data is transferred to a third country or to an international organisation, the Data Subject has the right to be informed of the appropriate safeguards we implement relating to the transfer;

The access request can be in any form – verbally or in writing and we must verify the data subject's identity before we provide any information. We will provide a copy of the Personal Data undergoing processing. For any further copies requested by the Data Subject, we may charge a reasonable fee based on administrative costs and we may refuse to respond, where a request is manifestly unfounded or excessive, in particular because it is repetitive. Where the Data Subject makes the request by electronic means, and unless otherwise requested by the Data Subject, we will provide the information in a commonly used electronic form.



## 10.2 Rights to object to processing

A relevant Data Subject may have his or her Personal Data erased, rectified, amended or completed as specified below:

- a) **Deletion:** right to ask us to delete Personal Data we hold about the Data Subject though we may need to keep all or part of such data in accordance with applicable Data Protection Legislation (e.g. if we need to keep all or part of this Personal Data to comply with our legal obligations, for record keeping or to keep providing you any of our services);
- b) **Rectification:** entitled to have any inaccuracies in the information we hold about him or her corrected;
- c) **Withdraw consent:** right to withdraw consent to any particular use of his or her Personal Data;
- d) **Information:** right to be informed of the use to which the Personal Data is put;
- e) **Restriction:** under certain circumstances specified by Data Protection Legislation, a Data Subject has the right to request us to restrict the processing of his or her Personal Data, or we may restrict the processing of such data (e.g. if a Data Subject claims his or her Personal Data is inaccurate or objects to the processing of such Personal Data and we are considering the request, or if processing is unlawful and the Data Subject opposes erasure and request restriction instead, etc.);
- f) **Object:** right to object to our processing of the Data Subject's Personal Data based: (i) on our legitimate interests or the performance of a task in the public interest; (ii) direct marketing (including profiling); (ii) processing for purposes of scientific/historical research and statistics;
- g) **Portability:** right to request us to provide the Data Subject with his or her Personal Data in a structured, commonly used and machine readable form and to ask us to transmit the data directly to another organisation if this is technically feasible;
- h) Right to require a data controller to ensure that no decision significantly affecting the Data Subject is based solely on the automated processing of his Personal Data for the purpose of evaluating matters relating to him or her (such as work performance, creditworthiness, reliability or conduct).

## 11. Data security

- 11.1 Will process the Personal Data 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.
- 11.2 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. Personal Data will only be transferred to a Processor if he



agrees to comply with those procedures and policies, or if he puts in place adequate measures himself.

11.3 We will maintain Personal Data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows:

- a) Confidentiality means that only people who are authorised to use the Personal Data can access it;
- b) Integrity means that Personal Data should be accurate and suitable for the purpose for which it is processed;
- c) Availability means that the Data Users should be able to access the Personal Data if they need it for authorised purposes. Personal Data should therefore be stored on the Osborne central computer system instead of individual PCs.

11.4 Security procedures include:

- a) Entry controls. Any stranger seen in entry-controlled areas should be reported;
- b) Secure lockable desks and cupboards. Desks and cupboards should be kept locked if they hold confidential information of any kind (Personal Data is always considered confidential);
- c) Methods of disposal. Paper documents should be disposed through a company specialised in disposing of confidential documents which is able to certify that the documents have been disposed safely. Digital storage

devices should be physically destroyed when they are no longer required;

- d) Equipment. Data Users must ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.

## 12. Transferring Personal Data to a country outside the EEA

12.1 We may transfer any Personal Data we hold to a country or an international organisation outside the EEA, provided that one of the following conditions applies:

- a) where the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection; or
- b) we may transfer Personal Data to a third country or an international organisation only if we provide appropriate safeguards, and on condition that enforceable Data Subject rights and effective legal remedies for Data Subjects are available.

12.2 In the absence of an adequacy decision, or of appropriate safeguards, a transfer or a set of transfers of Personal Data to a third country or an international organisation take place only on one of the following conditions:

- a) the Data Subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the



Data Subject due to the absence of an adequacy decision and appropriate safeguards;

- b) The transfer is necessary for one of the reasons set out in the Data Protection Legislation, including the performance of a contract between us and the Data Subject (or the implementation of pre-contractual measures taken at the Data Subject's request), or to protect the vital interests of the Data Subject;
- c) The transfer is necessary in order to protect the vital interests of the Data Subject, is legally required on important public interest grounds or for the establishment, exercise or defence of legal claims;
- d) The transfer is authorised by the relevant data protection authority under the specific requirements of the Data Protection Legislation;
- e) The Personal Data we hold, may also be processed by staff operating outside the EEA who work for us or for one of our suppliers. That staff may be engaged in, among other things, the fulfilment of contracts with the Data Subject, the processing of payment details and the provision of support services;
- f) Disclosure and sharing of Personal Data: we may share Personal Data we hold with any member of our group, which means our subsidiaries, our ultimate holding company and its subsidiaries, as defined in section 1159 of the UK Companies Act 2006.

### 13. Disclosure of Personal Data we hold to third parties

13.1 We may also disclose Personal Data we hold to third parties:

- a) 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;
- b) 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;
- c) 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 employees, customers, or others. This includes exchanging information with other companies and organisations for the purposes of fraud protection and credit risk reduction;
- d) We may also share Personal Data we hold with selected third parties for the purposes set out in the Schedule 1.

### 14. Dealing with subject access requests

14.1 Data Subjects must submit a formal request to access the information we hold about them. This can be made verbally or in writing. Employees who receive a written or verbal request should forward it to the DPO at [dataprotection@osborne.co.uk](mailto:dataprotection@osborne.co.uk) immediately.



14.2 The Data Subject requests from Employees must be made verbally or in writing to the People Team.

## 15. Changes to this policy

15.1 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.

## 16. Responsibilities

### Managers

16.1 Managers at all levels have responsibility for the type of Personal Data collected, how they use it and for communicating this to anyone in their team.

### Everyone

16.2 Everyone is required to be mindful of their personal responsibility for data protection, for example, ensuring that all paperwork containing Personal Data relating to a named individual must be locked away in a secure cabinet. There is a risk in sending confidential information by email or fax. Where the communication of such information by email is essential then this must be protected by a password agreed with the intended recipient.

16.3 Examples of paperwork which may contain Personal Data:

- a) Personnel Record Sheet;
- b) Pension Choices Opt In form;
- c) Life Assurance beneficiary;
- d) Nomination forms;

- e) Accident report forms;
- f) Recruitment forms;
- g) Resident profile forms (QA1);
- h) Job sheets / Job reports.

16.4 Everyone is:

- a) Required to keep the People Team informed of any changes to personal details which are relevant to the employment relationship;
- b) Required to follow the IT Policy including security of data;
- c) Responsible for ensuring any Personal Data they Process in the course of their work is in accordance with Data Protection Legislation and with this Policy.

### The People Team

16.5 The People Team are required to:

- a) Send a holding response to the relevant Data Subject and try to respond to Personal Data requests (Data Subject Rights) from a Data Subject within 30 days (unless this is not reasonably feasible) and in accordance with this Policy and other applicable Osborne procedures;
- b) Respond to third party requests for information in line with the guidelines given above and with other applicable Osborne procedures. Some requests, such as from mortgage companies, letting agents, loan



arrangers and child support agencies will be passed to the payroll department;

## 17. Statutory Role

17.1 The Group Finance Director has overall responsibility for ensuring the Group complies with the Data Protection Legislation and will ensure that guidance, policies and procedures around Personal Data processing are kept up to date. The Data Protection Officer is responsible to monitor and audit the Group's application of the Data Protection Legislation and this policy and will also liaise with the Information Commissioners Office as necessary.

## 18. Breaches Report Procedures

- 18.1 If you become aware or suspect there has been a breach of the Data Protection Legislation or this policy, please report immediately to the Data Protection Officer at [dataprotection@osborne.co.uk](mailto:dataprotection@osborne.co.uk).
- 18.2 If you become aware or suspect there has been a Personal Data breach (including any data loss) please report immediately to the Data Protection Officer at [dataprotection@osborne.co.uk](mailto:dataprotection@osborne.co.uk). Osborne's data breach report procedures must be followed.
- 18.3 Examples of data breaches/loss:
- a) Loss or theft of data or IT equipment/ memory stick, laptop or mobile device on which Personal Data is stored;
  - b) Unauthorised access to Personal Data Processed by us;

- c) Credentials (user name and passwords) compromised;
- d) Ransomware attacks;
- e) Inappropriate access controls allowing unauthorised use;
- f) Unforeseen circumstances such as fire or flood;
- g) Hacking attack; and
- h) Blagging - where information is obtained by deceiving the organisation who holds it.

Policy Number: CS-CP-006  
4<sup>th</sup> March 2020 – V1.10



## POLICIES & STATEMENTS

### Data Protection and Privacy



#### Schedule 1

Type of data	Type of Data Subject	Lawful Basis for Processing	Type of processing	Purpose of processing
Basic Personal Information relating to customers (including housing association tenant data)	Mainly direct customers of our partners (such as local councils) for whom we carry out work	Consent; Performance of a contract	Maintaining database of customers, recording calls to call centres	To provide maintenance services for data subjects in accordance with our contractual obligations
Basic Information relating to employees and subcontractors (including bank account information and national insurance numbers)	Employees and sub-contractors	Performance of a contract	Maintaining databases; sharing information with service providers and contractors	Performance of employment contract or sub-contract
Health information relating to safety-critical personnel	Employees or sub-contractors (safety-critical)	Protecting the vital interests of the data subjects and others	Maintaining databases	Ensuring safety at worksites
CCTV and on-boarding at worksites	Name, address, National Insurance Number/passport number, video	Protecting the vital interests of the data subjects and others	Maintaining databases	Ensuring safety at worksites