

Data Protection Policy

Purpose

This Policy sets out our commitment to protecting personal data and how Orwell implements that commitment in line with the legal requirements contained in the UK General Data Protection Regulation (UK GDPR) and The Data Protection Act 2018 (DPA2018). Orwell is committed to complying with all UK Data Protection legislation.

The Board has overall responsibility for compliance with data protection legislation and this Policy.

The Assistant Director of IT and Head of Governance acting as Data Protection Officer will have operational responsibility for the delivery of this policy. To ensure that Data Protection is embedded throughout the business, support will be provided by an Information Governance Steering group.

Due to the quantity and sensitivity of data processed by Orwell, it is considered necessary to appoint a Data Protection Officer.

All employees, Board members and third parties working on behalf of Orwell are responsible for complying with all UK Data Protection legislation and this Policy.

Legal Obligations

Orwell will comply with all relevant UK legislation.

Policy Statement

Orwell is committed to respecting the rights and privacy of individuals.

Orwell will ensure that personal data is processed in a manner compliant with UK legislation and will appropriately manage risks associated with the processing of personal data.

Orwell will establish an open and transparent environment in which Data Subjects are in control of their personal data and are fully informed of their rights and the legal basis for which their data may be used. Orwell will embed Data Protection principles in all business related activities.

This Policy applies to all personal data that Orwell process on behalf of Data Subjects.

Data Protection – Policy

During all decision making on processing personal data, Orwell will uphold the principles defined in Article 5 of UK GDPR:

- Only process personal data lawfully and fairly.
- Declare to Data Subjects the purpose for which it is processed.
- Only use it for the purpose declared.
- Only process the minimum amount of personal data for the purpose.
- Ensure that data is accurate.
- Only keep it for as long as necessary for the purpose.
- Personal data will be kept secure and treated as confidential.

As a Data Controller, Orwell will demonstrate compliance with the principles above.

All personal data processed must have a legal basis as defined in Article 6 of UK GDPR. In the case of Special Category Data, there must be an additional legal basis defined in Article 9 of UK GDPR. At the point of collecting personal data, the legal basis will be explained to the Data Subject, and they will be notified about their rights and given details about how their data will be used. Where personal data is provided by a third-party, the Data Subject will be informed as legally required.

Orwell will process special category data and criminal convictions and offences data. The legal basis for processing this data will be from the applicable grounds in Schedule 1 of the Data Protection Act 2018.

The UK GDPR and the Data Protection Act 2018 contain a number of exemptions or restrictions which allow Orwell to process information outside of the “usual” confines of the law. Such exemptions include, but are not restricted to:

- The prevention, detection or prosecution of criminal offences;
- Taxation, public health or social security purposes;
- The protection of judicial independence and judicial proceedings;
- Matter of public security, national security or defence;
- The safeguarding of children or individuals at risk.

If the legal basis for processing data is Consent from the Data Subject, this must be informed, freely-given, specific and unambiguously collected. It may be withdrawn at any time and a clear set of procedures will be available for Data Subjects to exercise this right. Data Subjects under 13 years of age will require Consent from a parent or guardian.

Personal data will be processed in accordance with the legal basis as explained to the Data Subject and they will be reminded to inform Orwell of any changes to their personal data.

If Orwell’s legal basis for processing is legitimate interest, a Legitimate Interest Assessment will be undertaken.

Orwell will maintain a data retention policy with associated schedule for the erasure and destruction of personal data. For paper documents containing personal data, this must be subject to destruction through our confidential waste disposal methods.

Orwell will respect the rights of Data Subjects and how individuals can exercise these rights is detailed within Orwell’s Privacy notice. This includes:

- the right to be forgotten;
- the right to object to processing;
- the right of data portability;
- the right of access;
- the right of rectification if data is incorrect;
- the right to be informed; and
- the right to restrict processing.

Orwell will comply with individuals’ rights to access their personal data as detailed in Orwell’s Subject access request procedure.

If Orwell undertakes profiling and/or automated decision-making, Orwell will ensure that in addition to the principles above, that:

- Additional checks are in place for profiling/automated decision-making systems to protect any vulnerable groups including children;
- A DPIA is completed to consider and address the risks before Orwell starts any new automated decision-making or profiling;
- Our customers are informed about the profiling and automated decision making processes, what

- information Orwell uses to create the profiles and where this information originates from; and;
- Anonymised data will be used in our profiling activities.

Orwell upholds the principle of data protection by design and default. Prior to any new processing activities or technology changes involving personal data the project lead must complete a screening process that establishes whether a full Data Protection Impact Assessment (DPIA) is required. Where there is a high risk to the rights and freedoms of data subjects, a DPIA will be undertaken by the project lead. The DPIA will be reviewed and approved by the Data Protection Officer or Assistant Director of IT and any risks will be managed accordingly. The outcome will be documented to demonstrate legal and regulatory compliance.

Orwell has established risk management processes in place to manage and mitigate data protection risks. Where appropriate, such risks and significant breaches are reported to the Executive team and Board.

As a Data Controller, Orwell is accountable for the data processed and any processing undertaken by third parties acting on Orwell's behalf. Orwell will ensure that Data Processors are subject to contract management.

All contracts with Data Processors will include a compliance clause to enforce control over the use of sub-processors. At the procurement selection stage and then periodically through contract management Orwell will assess the risk presented by a Data Processor.

Orwell will only share data with data processors or other data controllers (joint controllers) where a data sharing agreement, or a contract with clear data processing requirements and appropriate technical and physical security measures are in place. Data sharing arrangements will be reviewed periodically or where there is a significant change to process or associated risks.

Orwell will keep records to demonstrate compliance with Data Protection legislation.

To ensure that employees are aware of and understand their responsibilities when processing personal data, Orwell will deliver training and awareness programmes covering legislation, compliance, risk and other matters relating to data protection and privacy.

Orwell will maintain a central record of CCTV cameras in accordance with best practice. All CCTV will be managed in line with Orwell's CCTV Policy.

All breaches and near-misses will be investigated using a risk based approach by the Assistant Director of IT or the Head of Governance in line with our data breach procedure.

The selection of ICT infrastructure and applications will follow the Information Security Policy.

Personal data will not be transferred to countries outside the United Kingdom or European Union except where such countries have been determined to have adequate data protection provisions through a European Commission adequacy decision or there is a set of adequate safeguards with contractual terms as approved by the Information Commissioners Office (ICO) or the European Commission. Before a decision is made to transfer data outside of the UK or EU, a full assessment will be undertaken by the Assistant Director of IT and Head of Governance, with approval provided by the Executive team.

Orwell is not a public body and therefore is not directly obligated to abide by the requirements of the Freedom of Information Act 2000. However, where Orwell is delivering a service on behalf of a public body, employees should be aware that any data processed in relation to delivery of the service could be made public under a request of this nature.

Policy definitions

Anonymisation – keeping a record but clearing the personal data.

Breach – an incident which has highlighted non-compliance with the General Data Protection Regulation.

Data Controller – an organisation, such as Orwell Housing, that controls the flow of personal data collected by it about Data Subjects.

Data Processor – an organisation working under contract with a Data Controller on their behalf that processes personal data.

Data Sharing Agreement – Data Processors must only act on the written instructions of the Data Controller. Standard clauses are part of the contract between the Data Controller and the Data Processor. An agreement for the sharing of personal data amongst Data Controllers (as opposed to Data Processors, an example being where Orwell share data legally with Local Authorities or Police).

Data Protection Officer (DPO) – an independent expert in data protection whose role is to monitor internal compliance, inform and advise on your data protection obligations, provide advice regarding the impact of processing personal data and act as a contact point for data subjects and the Information Commissioner.

Data Subject – an individual whose personal data is being processed.

Data Protection Impact Assessment (DPIA) - used to identify privacy or Data Protection concerns before implementing new ways of processing personal data, and/or technology changes.

Near-miss - an incident where a breach would have occurred except for an unexpected action or set of circumstances which prevented it.

Personal data – as defined in Article 4 of GDPR means any information relating to a person, identified or identifiable from that data either directly or indirectly, in an electronic or paper structured filing system

Privacy Notice – A statement describing how Orwell collects, uses, stores and shares personal data.

Pseudonymisation – replacing personal data with an identifier that cannot be used to identify the Data Subject except from a separate limited-access set of records.

Special category data – this is personal data that needs more protection because it is sensitive – it is prescribed as personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data (where used for identification purposes), data concerning health, a person's sex life; or a person's sexual orientation. Orwell also considers criminal convictions and offences data to be special category data.

Sub-processor – an organisation which processes data on behalf of a Data Processor with whom Orwell have shared personal data.

Data Protection Policy Breach

Failure to adhere to this policy is a disciplinary offence, which may be considered to be serious/gross misconduct.