Data Protection Policy

May 2018

Led by:	Liz Chaffe – Senior Legal Executive/Data Protection Officer
Written by:	Bethany Paliga – Solicitor - Forbes Solicitors Erica Sanderson – Business Assurance Officer
Agreed on:	17th May 2018
Agreed by:	Group Audit & Risk Committee
Updated:	
To be reviewed:	May 2019

Contents

1. Our 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 collect, store and process personal data about our customers, employees, suppliers, and other third parties and we recognise that the correct and lawful treatment of this data will maintain confidence in our business activities.

1.2 Ongo Partnership Ltd. and all of our subsidiaries are responsible for collecting, processing, storing and safe-keeping of personal data about our customers, employees, suppliers and other third parties.

1.3 We manage personal information in accordance with the General Data Protection Regulation (EU) 2016/679 ("The GDPR) and the Data Protection Act 2018 ("The DPA")

1.4 The GDPR and DPA controls how personal information we hold about our customers and employees is used. Everyone using the data has strict rules to follow; "Data Protection Principles". We must make sure personal information is:

- used fairly, lawfully and in a transparent manner;
- Collected for specified, explicit and legitimate purposes and not processed in a manner which is incompatible with those purposes;
- Adequate, relevant and limited to what is necessary in relation to the purpose the data is being used for;
- Accurate and, where necessary, up to date;
- kept for no longer than is necessary;
- Kept securely so that data is protected against unauthorised use, accidental loss, destruction or damage.

2. It applies to…

2.1 This policy applies to all employees of Ongo Partnership Ltd., its subsidiaries and our customers. Compliance with this policy is mandatory and any breach of this policy may result in disciplinary action.

2.2 Any external organisation and/or person(s) working on behalf of ongo and its subsidiaries are required to comply with this policy.

2.3 All managers are responsible for ensuring all staff comply with this policy and need to implement appropriate practices, processes, controls and training to ensure compliance.

2.4 The Data Protection Officer ('DPO') is responsible for overseeing this policy and developing related policies and guidelines as applicable. The DPO post is held by

[Liz Chaffe]. The DPO can be contacted by calling 01724 298772 or via e-mail - liz.chaffe@ongo.co.uk.

2.5 Please contact the DPO with any questions about this policy, the DPA or if you have any concerns that this policy is not being or has not been followed.

2.6 You must always contact the DPO in the following circumstances:

- if there has been a data protection breach;
- if you are unsure that you have a lawful basis to use personal data in a particular way;
- whenever you are engaging in a new activity which may affect privacy rights of individuals;
- if you need to rely on or capture consent;
- if you need to draft a privacy notice;
- if you are unsure about how long you should keep personal data for;
- if you are unsure about what security measures you need to implement to protect personal data;
- if you need any assistance dealing with any rights invoked by an individual;
- if you need help with any contracts or other areas in relation to sharing personal data with third parties; or
- if you need to transfer personal data outside of the European Economic Area (EEA) (The **EEA** includes **EU** countries and also Iceland, Liechtenstein and Norway. It allows them to be part of the **EU** 's single market[1].

3. Because we want to...

3.1 Ensure that:

- we are legally compliant;
- individuals and Ongo are protected;
- all controls are in place to avoid any data protection breaches; and
- all staff, customers, suppliers/contractors and other stakeholders understand what Data Protection is and how it is managed across Ongo.

4. Our legal basis for processing personal data...

4.1 Personal data must be processed lawfully, fairly and in a transparent manner.

4.2 You may only collect, process and share personal data fairly and lawfully and for specified purposes. The DPA restricts our actions regarding personal data to specified lawful purposes. These restrictions are not intended to prevent

[1] Taken from https://www.gov.uk/eu-eea

processing, but ensure that we process personal data fairly and without adversely affecting individuals.

4.3 The GDPR and the DPA allows processing for specific purposes, these include:

- The individual has given their consent;
- The processing is necessary for the performance of a contract;
- To meet our legal obligations;
- To protect an individual's vital interests;
- The processing is necessary for the performance of a task carried out in the public interest; and
- The processing is necessary for our legitimate business interests, provided that those interests are not overridden by the rights and freedoms of the individual.

5. What information we collect...

5.1 As a business we may collect, process and store information such as:

- Customer names, dates of birth, National Insurance Numbers, photographs, contact details and contact preferences;
- Equality and diversity information about our customers;
- Applications for housing, including references, pre-tenancy assessments, housing history and income details;
- The details of other individuals living in our properties;
- Financial details including bank details, benefit support, rent account details and income and expenditure assessments;
- Physical and mental health details;
- Details of any criminal convictions or legal proceedings;
- Complaints of anti-social behaviour;
- Complaints about our services;
- Repair logs;
- Details of any support received by customers including care packages and plans and details of support providers;
- CCTV images.

5.2 As an employer, we may collect, process and store information such as:

- Staff names, contact details, dates of birth, National Insurance numbers, tax code, identification documents and photographs, ethnicity;
- Disability information;
- Bank details;
- DBS checks;
- Attendance, sickness and absence records;
- Details of education and qualifications;
- Work experience and previous job history;

- Employment terms and conditions;
- HR records including performance and workplace monitoring;
- Details of any accidents;
- Training records;
- Any disciplinary details;
- CCTV images.

6. Why we collect this information…

6.1 We may process this information to carry out our business activities. This includes:

- Letting, renting and leasing properties;
- Administering waiting lists;
- Carrying out research;
- Administering housing and property grants;
- Providing associated welfare services, advice and support;
- Maintaining our accounts and records; and
- Supporting and managing our employees, agents, and contractors.

6.2 Use personal information to respond more efficiently and accurately to enquiries, provide services to our customers, manage relationships with our customers and use the information to:

- Notify customers of changes we are planning to make to service provision;
- Help us improve our services; or
- Inform customers about our services or events.

6.3 Apply markers to the customer information we hold (for example, in relation to a customer's vulnerabilities or health status) to enable us to tailor and deliver our services appropriately and to comply with our health and safety obligations to our staff.

6.4 The DPA requires us to provide detailed, specific information to individuals depending on whether the information was collected directly from the individuals themselves or received from elsewhere. Such information must be provided through appropriate privacy notices which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that an individual can easily understand them.

6.5 Whenever we collect personal data directly from individuals, including for HR or employment purposes, we will provide the individual with all the information required by the DPA including the identity of the data controller and DPO, how and why we will use, process, disclose, protect and retain that personal data through a privacy notice which must be presented when the individual first provides the personal data.

6.6 A copy of our privacy notices that are to be issued to customers and staff when they first provide their personal data are attached at [Appendix 1] and [Appendix 2]. A copy of our privacy notices that are issued to users of our website and portal app are also attached at [Appendix 3] and [Appendix 4].

7. We will…

7.1 We will not use personal data for new, different or incompatible reasons from that disclosed when the information was first obtained unless we have informed the individual of the new reasons for using their personal data and they have consented where necessary.

7.2 We will make sure that personal data is adequate, relevant and limited to what is necessary in relation to the reasons for which it is obtained.

7.3 We will only collect, use and process personal data when performing our job duties requires it. We cannot collect, use or process personal data for any reason unrelated to our job duties.

7.4 We will ensure that when personal data is no longer required, it is deleted or anonymised in accordance with our Data Retention Policy. All staff are required to comply with our Data Retention Policy.

7.5 Comply with the Law when required to undertake Disclosure and Barring Service checks in line with our DBS Procedure.

8. Security…

8.1 Personal data must be secured by appropriate technical and organisational measures against unauthorised or unlawful processing and against accidental loss, destruction or damage.

8.2 We will always protect personal data. In particular:

- We aim to make sure staff and board members do not misuse any confidential information or pass on this information improperly to a third party;
- We protect personal information by applying technical measures, implementing policies, training staff and carrying out checks on practice.
- Where paper files and records containing personal information are unavoidable, we shall store these in secure cabinets.

- Any information on our computer system is secure, accurate, relevant and necessary. The personal data held on mobile electronic devices is minimised and appropriate security methods implemented against unlawful or unauthorised access;
- Users who have access to our online services (personal information, rent account information or repair details) can only view their own data;
- All data held for our online platform is secure.

8.3 All staff must follow all our procedures and technologies we put in place to maintain the security of all personal data from the point it is collected to the point it is destroyed. For further details please refer to our ICT Acceptable Use Policy.

8.4 All staff must comply with all applicable aspects of our Data Security Guidance and our ICT Acceptable Use Policy and not attempt to circumvent the administrative, physical and technical safeguards we implement and maintain in accordance with the GDPR and the DPA and relevant standards to protect personal data.

9. CCTV...

9.1 We use CCTV in various locations around Ongo premises to ensure they remain safe.

9.2 We will adhere to the ICO's Code of Practice for the use of CCTV and our CCTV Procedure.

9.3 We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by signs explaining that CCTV is in operation.

9.4 We will make sure we keep the recorded images secure and delete them when they are no longer necessary in accordance with our CCTV Procedure.

10. Photographs...

10.1 As part of our activities, we may take photographs and record images of individuals within our offices and communities where we consider it is necessary and appropriate to do so.

10.2 We will seek the necessary consent for photographs to be taken of individuals for our communication, marketing and promotional materials including:

- For use within our offices on notice boards, magazines, brochures, newsletters etc

- For use outside of our offices by external agencies such as a photographer, newspaper, campaigns etc; and
- For use online.

11. Data Protection Breaches…

11.1 If you know or suspect that there has been a potential data protection breach, do not attempt to investigate the matter yourself. You must immediately contact the DPO and follow our Data Breach Procedure. You must preserve all evidence relating to the potential data protection breach.

11.2 We will investigate all reports of potential data protection breaches and provide reports of the investigations and outcomes to the relevant boards and/or committees, including lessons learnt reports.

11.3 We will report all data protection breaches to the Information Commissioner's Office within 72 hours when necessary to do so. We have put in place procedures to deal with any suspected data protection breaches and will notify individuals and/or the Information Commissioner's Officer where we are legally required to do so. Please see our Data Breach Procedure for further guidance.

11.4 We will notify those whose personal data has been breached at the earliest opportunity where it is appropriate to do so.

12. Sharing personal information…

12.1 We will not normally share personal data with anyone else. However, there a certain circumstances where we will be required to share personal data with other organisations and we will comply with the GDPR and the DPA when disclosing this information.

12.2 We will share data withal members of the Partnership, affiliated organisations and contractors working for us, where the information relates to warnings logged on our systems in order to safeguard staff safety.

12.3 If we or any of our contractor staff become aware of a staff safety issue with regards to one of our tenants or residents, we will share that information with the appropriate teams and/or individuals to ensure the safety of all concerned.

12.4 We may share personal information in some circumstances with other agencies. We will obtain necessary consent before referring customers to another service provider.

12.5 Sometimes we share personal information with our suppliers and/or contractors who enable us to provide services to our customers – e.g. our Gas Servicing. The data shared is limited to the specific information the supplier requires in order to carry out their service as well as any additional information that ensures we fulfil our Health & Safety obligations to the people carrying out the work. We will ensure that our suppliers handle this data correctly through the contract terms, checking their GDPR/DPA Compliance as part of our procurement process.

12.6 We will be responsible for the fair and lawful processing of personal data shared with other third parties. We make sure this occurs through setting data sharing agreements either in contracts or as stand alone agreements.

12.7 We will share personal data with law enforcement and government agencies or public bodies where we are legally required to do so. Examples include:

- The prevention or detection of crime and/or fraud;
- The apprehension or prosecution of offenders;
- The assessment or collection of tax owed to HMRC;
- In connection with legal proceedings;
- Where the disclosure is required to satisfy our safeguarding obligations; or
- Research and statistical purposes.

12.8 We may share information where necessary with emergency services and local authorities where this is necessary for them to respond to an emergency situation that affects any of our customers or employees.

12.9 Where it is required or necessary in accordance with the DPA, we may share information with:

- Current, past or prospective employers;
- Family, associates and representatives of the person whose personal data we are processing;
- Educators and examining bodies;
- Suppliers and service providers;
- Financial organisations;
- Central government;
- Auditors;
- Survey and research organisations;
- Other housing associations, trusts or local authorities;
- Trade unions and associations;
- Health authorities;
- Enquirers and complainants;
- Security organisations;

- Health and social welfare organisations;
- Professional advisers and consultants;
- Homes England;
- Probation services;
- Charities and voluntary organisations;
- Police forces;
- Courts and tribunals;
- Professional bodies;
- Employment and recruitment agencies;
- Credit reference agencies;
- Debt collection agencies;
- Landlords;
- Press and the media.

13. Individual's Rights and Requests…

13.1 Individuals have rights when it comes to how we handle their personal data. These include rights to:

- withdraw their consent to processing at any time;
- receive certain information about the data controller's processing activities;
- request access to their personal data that we hold;
- prevent our use of their personal data for direct marketing purposes;
- in certain circumstances, to ask us to erase personal data;
- to rectify inaccurate data or to complete incomplete personal data;
- in certain circumstances to restrict the processing of their personal data;
- challenge processing which has been justified on the basis of public interest;
- request a copy of agreements under which personal data is transferred outside of the EEA;
- object to decisions based solely on automated decision making or profiling;
- prevent processing that is likely to cause damage or distress;
- in certain circumstances, be notified of a data protection breach;
- make a complaint to the Information Commissioner's Officer; and
- in limited circumstances, ask for their personal data to be transferred to a third party in a structured, commonly used and machine readable format.

13.2 Staff must immediately forward any request to exercise data protection rights which they receive to the DPO and comply with our Data Subject Access Procedure, Data Portability Procedure or Right to Erasure Procedure where applicable.

14. Making sure we do what we say...

14.1 We must ensure we have appropriate technical and organisational measures in place, to ensure compliance with the data protection principles. These include:

- appointing a suitably qualified DPO;
- implementing privacy by design when processing personal data and completing privacy impact assessments where processing presents a high risk to rights and freedoms of individuals;
- integrating data protection into internal documents including this policy, any related policies and any privacy notices;
- regularly training members of staff on the DPA, this policy, any related policies and any other data protection matters. We will maintain a record of training attendance by members of staff; and
- regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance.

14.2 The Data Protection Working Group (for roles and responsibilities see Appendix 5) will ensure compliance with the General Data Protection Regulation (EU)2016/679 and the Data Protection Act 2018 and that our policy and procedures are followed.

14.3 The designated DPO will manage and monitor all reported breaches and report to the Group Audit & Risk Committee on all matters and the ICO when appropriate.

14.4 The VfM & Procurement Manager and Contracts Managers are responsible for ensuring suppliers comply with this policy and that, when personal data will need to be transferred to a contractor, the details will be written clearly into the contracts.

14.5 All staff will complete mandatory data protection related training as and when required.

15. Other things to bear in mind...

15.1 This policy also links to our:

- ICT Acceptable Use Policy;
- Data Retention Policy;
- Data Protection Breach Procedure;
- Subject Access Request Procedure;
- Data Portability Procedure;
- Right to Erasure Procedure;
- Privacy Impact Assessment Procedure;

- Data Security Guidance;
- BYOD Guidance;
- DBS Procedure;
- CCTV Procedure;
- Media Policy;
- Safeguarding Policy & Procedures;
- Procurement Policies and Procedures.

15.2 The main piece of legislation relevant to this policy is the General Data Protection Regulation (EU) 2016/679 and the Data Protection Act 2018.

15.3 For absolute clarity, Ongo is not a public body and is therefore not required to comply with requests made under the Freedom of Information Act (2000) or the Environmental Information Regulations (2004), except where we are carrying out statutory duties on behalf of a local authority or other public body. We will however, seek to answer requests for information if asked, providing the information is not 'commercially sensitive'.

16. We'll look at this again...

16.1 In a year's time, or earlier should any changes to legislation or regulation occur.