ASTER GROUP

Data Protection, Privacy and Confidentiality Policy

Approved by:	Group Risk & Compliance Committee		
Effective date:	15/05/2018	**Review date:**	15/05/2020
Author & responsible officer:	Risk & Compliance Lead (Data Protection Officer)		
Status:	*Approved*	**Version:**	6.00
Supersedes:	Data Protection and Confidentiality Policy (v5) Customer Verification Policy Data Retention Policy		

1 Introduction

1.1 Aster Group is the data controller of the information that it collects and manages.
The lawful and ethical treatment of personal information by Aster is extremely important to the success of our business, to maintain the confidence of our customers, colleagues and other stakeholders.

1.2 Aster is committed to a policy of protecting the rights and privacy of individuals in accordance with the General Data Protection Regulations (GDPR) and the Data Protection Act 2018, jointly referred to in this policy as 'the Act'.

1.3 To deliver its purpose as a landlord, service provider, developer and employer, Aster needs to collect and process certain types of personal information. This may include, but is not limited to, personal information relating to customers, close friends and family of customers, potential customers, colleagues, employment applicants, board members, suppliers and others with whom it communicates.

1.4 The duty of confidentiality also extends to any sensitive commercial information relating to Aster or its associates.

Compliance Framework

1.5 Aster recognises the importance and benefits of complying with data protection legislation and the opportunities arising from a culture of strong data protection practice and a focus on privacy. Being clear, transparent and lawful in how personal data is processed will build stakeholder trust.

1.6 Aster will take into account the nature, scope, context and purposes of processing as well as the risks to the rights of individuals and will implement appropriate technical and organisational measures to meet the requirements of data protection legislation.

1.7 Compliance Obligations relevant to this policy include;

- General Data Protection Regulations (GDPR)
- Data Protection Act
- Privacy and Electronic Communications Regulations (PECR) (to be superseded by ePrivacy Regulations)
- Human Rights Act
- Equality Act

2 Definitions

2.1 **Personal data** – is any information relating to an identified or identifiable natural person. This is someone 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 person. It includes Aster's opinion of or intentions towards that person.

2.2 **Special categories** - racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health* or data concerning a natural person's sex life or sexual orientation.

*data concerning health means personal data relating to the physical or mental health of an individual including the provision of health care services, which reveal information about his or her health status.

The Act requires that data relating to criminal convictions is treated in the same way as special categories of data.

2.3 **Data Subject** - the identified or identifiable living individual to whom personal data relates.

2.4 **Processing** - an operation or set of operations which is performed on personal data, or on sets of personal data, such as:

- collection, recording, organisation, structuring or storage;
- adaptation or alteration;
- retrieval, consultation or use;
- disclosure by transmission, dissemination or otherwise making available;
- alignment or combination; or
- restriction, erasure or destruction.

2.5 **Data controller** – an organisation that determines the purposes for which and the manner in which any personal data is, or is to be, processed.

2.6 **Data processor** – an organisation who processes the data on behalf of the data controller.

2.7 **Personal data breach** - means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

2.8 **Conditions for processing** - Data controllers must have a legal basis for processing any data. The Act sets out the legal basis for processing. There are additional conditions for processing special categories of data.

2.9 **Surveillance** - A collective term for the systems and devices that monitor or record the activities of individuals, or both.

2.10 **Information Commissioners Office (ICO)** - is the supervisory body for data protection in the UK. It has a number of investigative and corrective powers, as enshrined in the Act.

3 Policy Statement

3.1 This policy forms part of an enabling Data Protection Framework that supports lawful processing and the proportionate and legitimate use of and sharing of information.

3.2 Aster will ensure that personal information is:

- processed lawfully, fairly and in a transparent manner in relation to individuals;
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with the original purposes;
- adequate, relevant and limited to what is necessary
- accurate and kept up to date;
- kept in a form which identifies data subjects for no longer than is necessary; and
- processed with appropriate security using technical and organisational measures.

3.3 Asters framework of Data Protection guidance will support colleagues to record how these principles have been applied to any on-going or new data processing activities.

3.4 This policy sets out how Aster will implement these principles.

4 Lawful conditions for processing

4.1 There are a number of lawful conditions for processing personal data. Aster will ensure it meets one of these conditions when processing and will record these in the Data Purposes Register.

4.2 Asters most common lawful basis for processing data is because it is necessary to enter into or perform a contract.

4.3 There will be occasions when it is in the legitimate interests of the organisation and/or the individual to process the data. When any new data is to be collected, and it relies on legitimate interest, an assessment will be carried out and recorded in the register.

4.4 Special categories data will usually require the explicit consent of the individual prior to processing. Limited exceptions may apply where processing is in relation to employment or it is in the public interest. Aster prefers to have consent even in these circumstances as it promotes transparency and also enables processing for wider business purposes than the limited exceptions permit.

4.5 Data should only be used for the purpose for which it was originally collected. If a new use is proposed for the data, we will carry out an assessment to ensure that the proposed purpose is compatible with the original and if appropriate, will advise the data subject/s of the new purpose.

5 Data Protection Impact Assessments (or Privacy Impact Assessment)

5.1 A data protection impact assessment (DPIA) is a process to help identify and minimise the data protection risks of a project.

5.2 Aster will complete a DPIA when implementing or making a change to a process or system that could have an impact on the privacy of individuals. A DPIA will always be completed when:

- using new technologies; and
- the processing is likely to result in a high risk to the rights and freedoms of individuals.

5.3 Any new project will be tested against a DPIA screening checklist to establish whether a full DPIA is required. Refer to the DPIA Guidance.

6 Sharing personal data with third parties

6.1 In the course of carrying out our business (known as our ‘legitimate interests’) Aster will need to share data with various types of third parties. Certain information may be processed and shared for legislative, regulatory or

monitoring purposes as laid down by statute. An example of this is payroll data to HMRC.

6.2 Outside of these purposes, where data is being shared on a routine basis to another organisation or under a provider contract, it is Aster's policy that written Agreements must be in place.

There are three types of Agreements we can use,

Data Sharing Agreements
Data Sharing Agreements are appropriate where Aster is routinely sharing and processing data about data subjects with other Data Controllers, e.g. Local Authorities, Utility Companies, the Police, staff Healthcare providers. Each will have a direct relationship with the data subject. The Agreement covers the data jointly processed by both organisations in delivering services with shared outcomes e.g social housing provision, healthcare support.

Data Sharing Protocols
Data Sharing Protocols are appropriate where multiple organisations sharing common purposes and customers (normally public services in a geographic County area) want a single data sharing approach. Where possible Aster will work proactively with local and public authorities to develop and be part of these in preference to Data Sharing Agreements.

Data Processing Agreements
Aster Group is the data controller of the information that it collects and manages. As data controller, Aster remains responsible for data when it is processed by other organisations on its behalf.
Data Processing Agreements are appropriate where Aster contracts a provider to deliver a service on its behalf, e.g. maintenance contractors, telecare providers, aids and adaptations installers. These are organisations (known as 'Data Processors') that do not have a direct contractual relationship with the data subject. Data Processors may only use the data in accordance with Asters instructions within the service contract.

6.3 **Appointment of Contractors and Suppliers**
Aster will only appoint service contractors and suppliers that can demonstrate appropriate data protection practices in accordance with data protection law. In each case, this due diligence must form part of the selection and appointment process. This is to give assurance that any third parties appointed are treating the personal data we share with the same level of protections as Aster would themselves.

6.4 **Family and friends**
Often, customers are happy for Aster to discuss their tenancy matter, service or other query with a family member or friend, but Aster recognises that

discussing their personal data must always be with their agreement. For one off instances, verbal or similar consent can often enable colleagues to then discuss a matter with a third party.
When the consent is on-going, an Authority to Disclose form (which can be found on the HUB) should be completed and the consent recorded on the customer record.

6.5 **Elected Representatives – Councillors and MPs**
The Act permits disclosure of personal information to elected representatives in certain circumstances. Refer to the Managing MP and Councillor enquiries procedure.

6.6 **Exceptional circumstances**
Exceptional circumstances in which personal information may be shared without prior knowledge or notice to the individual include:

- for the prevention and detection of crime or the capture or prosecution of the offender/s
- for the assessment or collection of tax or duty
- to comply with the law or a court order
- where there is a clear health & safety risk
- in connection with court proceedings or statutory action to enforce compliance with tenancy conditions
- anonymously, for statistical research purposes.

6.7 **Corporate and Commercial information**
Corporate and commercial information that is not in the public domain, will be treated as confidential and safeguarded accordingly.

6.8 Aster will not sell or dispose of for gain, any personal data.

7 Customer Verification

7.1 We have a responsibility to provide good customer service to our genuine customers, however, this responsibility has to be balanced with protecting confidentiality and guarding against fraud.

7.2 When personal information is being discussed, we will take steps to assure ourselves that

- the person we are talking to is who they claim to be
- they have the appropriate authority to discuss the matter.

The Customer Verification procedure sets out the steps to gaining this assurance.

8 Data Accuracy

8.1 Aster recognises the importance of ensuring the personal data we hold is accurate. To comply with this principle, we will

- take reasonable steps to ensure the accuracy of any new personal data obtained;
- ensure that the source of any personal data is clear;
- provide multiple avenues for data subjects to update their information when things change.

9 Data Minimisation and Retention

9.1 The Act requires that personal data should be limited to what is necessary for the purpose for which it is processed and kept in a form that identifies data subjects for no longer than is necessary.

9.2 Aster will only collect and retain the personal data it needs for each specified purpose and will periodically review whether aspects of data sets can be minimised so data subjects are no longer identifiable. Examples of when it would be appropriate to do this include satisfaction surveys or historical schedules of works.

9.3 The Data Management and Retention procedure provides guidance on Aster approach to disposal or retention of all data and includes a retention schedule.

9.4 Secure methods of disposal will be used when personal or sensitive commercial information is no longer required.

10 Surveillance

10.1 Surveillance monitors or records the activities of individuals, or both. An example of this is closed circuit television (CCTV). This means surveillance systems process personal data. As such, any surveillance undertaken by Aster must be carried out with all regard to Data Protection law and the code of practice for surveillance cameras and personal information. Further information is contained within the Surveillance Procedure.

11 Supporting data subject rights

11.1 Aster is committed to meeting the rights of individual data subjects under the Act. These are;

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability

- The right to object
- Rights in relation to automated decision making and profiling.

11.2 The right to be informed is closely linked to the principle of transparency and the provision of fair processing information. This information, called a 'Privacy Notice' is provided at key data collection interactions and at all times via the Aster website.

11.3 The most commonly exercised right is the right to access. In addition to fully supporting this right in its pure sense, Aster will endeavour to be open and transparent and will consider providing personal or property related information reasonably requested, outside of the constraints of a formal access request.

11.4 We will provide data subjects with information about their individual rights and how these can be exercised. The Supporting Individual Data Subject Rights procedure sets out in more detail how these rights apply in different circumstances to support appropriate management of requests.

11.5 Further information and the Privacy Notice can be found at www.aster.co.uk/privacy

12 Staff Training

12.1 Training in data protection is given to all employees:

- A self-learn module is completed by all office based employees within 3 months of joining and is repeated annually.
- Non-office based employees receive training via alternative means, tailored to their role.
- Role specific training is delivered such as enhanced customer verification training to contact centre employees.
- Regular awareness initiatives will support the formal learning.
- Technical data protection specialists will have access to the training required to ensure their knowledge remains up to date.

13 Information Security Events - Personal Data Breaches

13.1 A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that the term 'breach' is wider than the commonly recognised loss or inappropriate sharing of personal data.

13.2 All personal data security incidents (i.e. near misses) and breaches must be reported to the Risk & Compliance team. Please refer to the Information Security Events (Data Breach) procedure.

13.3 All breaches or suspected breaches will be investigated in accordance with this procedure. As required by the Act, any breach where it is likely to result in a risk to the rights and freedoms of individuals will be reported to the ICO. Aster will aim to do this within the required 72 hours' time period of Aster becoming aware of the breach.

13.4 If a breach is likely to result in a high risk to the rights and freedoms of individuals, the Act requires Aster to inform those concerned as soon as possible.

14 Direct Marketing

14.1 Direct Marketing is defined as 'the communication (by whatever means) of any advertising or marketing materials which is directed to particular individuals'. This definition covers any advertising or marketing material, including material promoting the aims of not-for-profit organisations.

14.2 The Privacy and Electronic Communications Regulations (PECR) provide rules about sending marketing and advertising by electronic means, such as telephone, email, text and picture or video message, or by using an automated calling system.

14.3 Consent is central to the rules on direct marketing and Aster will generally need an individual's consent before they can send marketing texts, emails or make calls to a number registered with the TPS.

14.4 Aster will give all regard to PECR and the future ePrivacy Regulations when undertaking any direct marketing. Further information can be found in the Direct Marketing Guidance.

15 Data Protection Officer

15.1 Aster has appointed the Risk & Compliance Lead as its Data Protection Officer. The responsibilities of this role include;

- informing and advising in relation to GDPR and other data protection laws;
- monitoring compliance with the GDPR and other data protection laws, and internally compliance with Asters data protection polices, including managing internal data protection activities; raising awareness of data protection issues, training staff and conducting internal audits;
- advising on, and monitoring, data protection impact assessments;
- cooperating with and acting as first point of contact for the ICO and for individuals whose data Aster processes.

15.2 When performing these tasks, Asters DPO will have due regard to the risk associated with processing operations, and takes into account the nature, scope, context and purposes of processing.

15.3 Aster will take account of the DPO's advice and the information they provide on Asters data protection obligations. Adequate resources will be provided to enable the DPO to meet their GDPR obligations, and to maintain their expert level of knowledge. If a decision is made at any time not to follow the advice given by the DPO, the reasons will be clearly documented to demonstrate accountability.

16 Roles and Responsibilities

16.1 Managers in each service area are responsible for;

- Understanding what information is held, changes made through addition or deletion, information flows and who has access and why.
- Understanding and addressing the risks to that information and ensuring it is used in ways that are compatible with the Act.

16.2 The Risk & Compliance team provide data protection advice and support.

16.3 The Data Protection Working Party considers data protection issues in general and provide support to the Data Protection Officer in the implementation of good data protection practices in their business area.

16.4 All employees are responsible for complying with data protection policy, procedure and guidance.

17 Policy and Procedure Links

Information Technology Security and Usage Policy
Data Protection Guidance
Customer Verification Procedure
Data Management and Retention Procedure
Surveillance Procedure
DPIA Guidance
Direct Marketing Guidance
Supporting Individual Data Subject Rights Procedure
Information Security Event (Data Breach) Procedure
IT Guidance