**Data retention policy**

|  |  |
| --- | --- |
| Version | *Final* |
| Prepared by | *Rebecca Outram (Housing Services Director)* |
| Approved by | *Directors Group* |
| Approved date | *21 July 2022* |
| Review dates | *July 2022* |
| Document Owner | *Housing Services Director* |
| Date of Next Review | *July 2024* |
| Lines of Defence/how is the document audited? | 1. *Approval by DG/Board/* 2. *Reviewed by Data Protection People* 3. *On Internal Audit programme* 4. *Create rules in our electronic storage system* |

Data Retention Policy

1.0 Scope

2.0 Equality and Diversity

3.0 Statement

4.0 Objectives

* 1. Policy
  2. Roles and Responsibilities
  3. Data Retention Periods
  4. End-of-life Data
  5. Compliance Monitoring

# Scope

* 1. The definitions within this policy are fully explained in the Data Protection Glossary (‘glossary’) at the back of this document, and are consistent with Article 4 of the GDPR.
  2. This policy applies to all personal data (see glossary for definition) held and processed by Hexagon, regardless of its format, including all forms of digital data (including e-mail), all forms of paper documents and all forms of archived data.
  3. These information assets are listed in the Information Asset Register.
  4. The policy reflects the requirements of the GDPR which states “Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed” (see glossary for definition of data subjects).
  5. The GDPR requires organisations to establish appropriate time limits for holding data.

# Equality and Diversity

* 1. An equality impact assessment ‘initial screening’ has been carried out which determined there to be no negative impact specific to those with protected characteristics.

# Statement

* 1. Hexagon, in line with both legislation and best practice, wishes to outline a consistent approach to data retention and disposal that respects the rights and freedoms of data subjects

# Objectives

* 1. This policy will ensure compliance with the GDPR and data protection legislation.
  2. The policy functions in conjunction with the Retention and end-of-life of Personal Data Procedure and the Data Retention Schedule to define how Hexagon retains each Information Asset containing personal data for a defined

period of time (the retention period) and what happens to it once that period expires.

# Policy

* 1. Roles and Responsibilities
     1. Information Asset Owners are responsible for applying this policy in respect of the information assets of which they are they owner.
     2. The IT Manager is responsible for ensuring that personal data held in digital form in centrally managed IT systems are retained and destroyed in compliance with this policy.
  2. Data Retention Periods
     1. Hexagon does not retain personal data for any longer than is necessary for the purposes for which that data is collects. Appropriate measures will be applied when that data reaches the end of its useful life (such as erasure or anonymisation).
     2. Hexagon may store data for longer periods if the personal data is processed (see glossary for definition) solely for archiving purposes in the public interest, for research, or for statistical purposes. This is subject to the implementation of appropriate technical and organisational measures to safeguard the rights and freedoms of data subjects.
     3. Information Asset Owners determine the retention period for personal data under their control, justification for the retention period and any sources used to inform that decision.
     4. The Data Protection Officer (DPO) maintains a schedule of data retention periods in the Data Retention Schedule which defines approved retention periods and end of life treatment. The Data Retention Schedule defines the reasoning for data retention periods. These may be influenced by different factors, including: statutory, regulatory, financial, industry sector best-practice or business considerations.
     5. The DPO approves all retention periods for personal data.
     6. Personal data is retained in accordance with Hexagon’s Retention and end-of- life of Personal Data Procedure.
     7. Retention periods for all information assets are made publicly known to the data subjects. Any changes to retention periods and/ or information assets results in an update to the published versions.
  3. End-of-life Data
     1. Personal data that has exceeded its retention period will be deleted, given a pseudonym or destroyed.
     2. Personal data that has exceeded its retention period but is the subject of a Data Subject Rights request, an investigation by the supervisory authority or legal proceedings will be retained until that request, investigation or proceeding is concluded. The DPO will advise in such a situation.
  4. Compliance Monitoring
     1. Hexagon ensures compliance with this policy by monitoring and auditing to ensure that personal data is managed, retained and disposed of accordingly.
     2. All retention periods (including any that are defined as indefinite retention) are reviewed annually and updated as appropriate under the guidance of the Information Asset Owner and the DPO.

**GLOSSARY OF TERMS**

1. **‘personal data’** means any information relating to an identified or identifiable natural person (‘**data subject’**); 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;
2. **‘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;
3. **‘restriction of processing’** means the marking of stored personal data with the aim of limiting their processing in the future;
4. **‘profiling’** means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;
5. **‘pseudonymisation’** means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;
6. **‘filing system’** means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;
7. **‘controller’** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;
8. **‘processor’** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;
9. **‘recipient’** means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. 2However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;
10. **‘third party’** means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;
11. ‘**consent**’ of the data subject means any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;
12. **‘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;
13. **‘genetic data’** means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;
14. ‘**biometric data’** means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;
15. **‘data concerning health’** means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;
16. **‘main establishment’** means:
    1. as regards a controller with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment;
    2. as regards a processor with establishments in more than one Member State, the place of its central administration in the Union, or, if the processor has no central administration in the Union, the establishment of the processor in the Union where the main processing activities in the context of the activities of an establishment of the processor take place to the extent that the processor is subject to specific obligations under this Regulation;
17. **‘representative’** means a natural or legal person established in the Union who, designated by the controller or processor in writing pursuant to [Article 27](https://gdpr-info.eu/art-27-gdpr/), represents the controller or processor with regard to their respective obligations under this Regulation;
18. **‘enterprise’** means a natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity;
19. ‘**group of undertakings’** means a controlling undertaking and its controlled undertakings;
20. ‘**binding corporate rules’** means personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity;
21. ‘**supervisory authority’** means an independent public authority which is established by a Member State pursuant to [Article 51](https://gdpr-info.eu/art-51-gdpr/);
22. **‘supervisory authority concerned’** means a supervisory authority which is concerned by the processing of personal data because:
    1. the controller or processor is established on the territory of the Member State of that supervisory authority;
    2. data subjects residing in the Member State of that supervisory authority are substantially affected or likely to be substantially affected by the processing; or
    3. a complaint has been lodged with that supervisory authority;
23. ‘**cross-border processing’** means either:
    1. processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or
    2. processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.
24. ‘**relevant and reasoned objection’** means an objection to a draft decision as to whether there is an infringement of this Regulation, or whether envisaged action in relation to the controller or processor complies with this Regulation, which clearly demonstrates the significance of the risks posed by the draft decision as regards the fundamental rights and freedoms of data subjects and, where applicable, the free flow of personal data within the Union;
25. ‘**international organisation’** means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries.
26. **‘data retention schedule’** defines approved retention periods and end of life treatment. The Data retention Schedule defines the reasoning for data retention periods. These may be influenced by different factors, including: statutory, regulatory, financial, industry sector best -practice or business considerations.
27. **‘**‘**Data retention period’** the length of time personal data is held.
28. ‘**information asset owner’** is responsible for ensuring that specific information assets are handled and managed appropriately.

.