

## Data Protection Policy

Document Owner	Head of Governance, Risk and Assurance
Prepared by	Data Protection Officer Policy Officer
Approved by	Board
Approved date	July 2024
Date of next review	July 2026
Monitoring, Auditing and Reporting	On Internal Audit programme

## 1 Scope and Aims

- 1.1 The UK GDPR applies to any UK organisation involved in the processing (the use of data - collecting, storing, recording, consulting, altering, disclosing, erasing, making available) and filing of data by either automated or non-automated means.
- 1.2 This policy applies to anybody who processes personal data for, or on behalf of, Hexagon and any external organisation or individuals with whom Hexagon shares or discloses personal data.
- 1.3 The policy will ensure compliance with all data protection legislation.
- 1.4 Hexagon's commitment to the protection of personal data, and the rights of those whose data it holds, will be ensured through upholding this policy.

## 2 Definitions

- 2.1 **Data 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 (but see section 6 of the 2018 Act).
- 2.2 **Data Processor** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
- 2.3 **Data Subject**: any living individual who is the subject of personal data held by an organisation.
- 2.4 **Data Process Owner**: the person responsible for the instigation or on-going maintenance of a data process or data processing operation.
- 2.5 **Personal Data** means any information relating to an identified or identifiable living individual.
- 2.6 **Identifiable living individual** means a living individual who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data or an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual;
- 2.7 **Special Categories of Personal Data** means any 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;

- 2.8 **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;
- 2.9 **Information Incident** means an identified occurrence or weakness indicating a possible breach of information security or failure of safeguards, or a previously unknown situation which may be relevant to the security of information;
- 2.10 **Information Security Event** an occurrence in a service, system, or network that indicates a possible breach of information security. This includes breaks in policy, failure of controls, or other previously unknown situations;
- 2.11 **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;
- 2.12 **Risk**: the chance of something happening, which will have an impact upon objectives. It is measured in terms of consequence and likelihood;
- 2.13 **Risk Management**: the culture, processes and structures that are directed towards the effective management of potential opportunities and adverse effects;
- 2.14 **Corporate Data**: Corporate data relates to any sensitive corporate information including meeting schedules, agendas and minutes of meetings; financial accounts; contracts; and organisational policies and procedures;
- 2.15 **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. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with domestic 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;
- 2.16 **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;
- 2.17 **Third Country** means a territory that is not the United Kingdom in the UK GDPR.

- 2.18 **Profiling** is any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person, or to analyse or predict that person's performance at work, economic situation, location, health, personal preferences, reliability, or behaviour. This definition is linked to the right of the data subject to object to profiling and a right to be informed about the existence of profiling, of measures based on profiling and the envisaged effects of profiling on the individual;
- 2.19 **Consent** 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;
- 2.20 **RoPA** means records of processing activities as required by Article 30 of the GDPR;
- 2.21 **Information Asset:** data or other knowledge that has value to an organisation.

### **3 Equality and Diversity**

- 3.1 Hexagon will implement this policy in line with our obligations under the Equality Act 2010. Data held about any of the protected characteristics must have a demonstrable purpose and should only be used to monitor and improve the service. This policy will clarify the way in which this data should be used and how we will oversee this.

### **4 Policy Statement**

- 4.1 Hexagon is committed to protecting the rights and freedoms of data subjects (any living individual who we have data for) whose information is collected and processed.
- 4.2 The policy will apply to all Hexagon's personal data processing functions, including those performed on personal data from residents, clients, employees, suppliers, contractors and partners, as well as any other sources.
- 4.3 Partners, processors and any third parties working with Hexagon are expected to have read, understood and comply with this policy.
- 4.4 No processor is authorised to process personal data on behalf of Hexagon without having first entered into a contract, which imposes obligations no less onerous than those to which Hexagon are committed and which gives Hexagon the right to audit as well as undertake other suitable data protection checks.

## 5 Roles and Responsibilities

- 5.1 Hexagon is the legal data controller under the Data Protection Legislation.
- 5.2 **Data Protection Working Group** oversees the implementation of UKGDPR of this policy and related procedures. The group meets at least quarterly.
- 5.3 **The Data Protection Officer (DPO)** is ultimately responsible for the monitoring of personal data within Hexagon and for ensuring that compliance with data protection legislation and good practice can be demonstrated. This function is currently fulfilled by a specialist Consultant.
- 5.4 **The DPO and the Head of Governance, Risk and Assurance** and those in executive, managerial and supervisory roles within Hexagon are responsible for developing good information handling practices, security aspects and arranging training within the organisation.
- 5.5 **The DPO and the Head of Governance, Risk and Assurance** have day-to-day responsibility for ensuring ongoing compliance with the data protection policy and legislation. Directors and managers also must ensure compliance in their areas of responsibility.
- 5.6 **The DPO** will take responsibility for the procedures associated with data protection and be available to any employees with queries regarding data protection. The DPO monitors and reports to the Head of Governance, Risk and Assurance in respect of compliance, the investigation of any security incidents, and maintenance of suitable records of processing activities. The DPO shall monitor the evolution of the Data Protection Legislation, case law, guidance, and codes of practice and incorporate relevant changes into the Organisation's policy in a change-controlled manner.
- 5.7 **Process Owner** – Process Owners are senior employees within each department who have been given direct responsibility for applying data protection principles over a particular process, contract or service. They are named on the Record of Processing Activities (ROPA). Their role is to understand:
  - 5.7.1 privacy risks to their information and protect them accordingly
  - 5.7.2 what information is held;
  - 5.7.3 what is added and what is removed;
  - 5.7.4 what information is moved;
  - 5.7.5 how long it should be kept for;
  - 5.7.6 who has access and for what purpose.

- 5.8 **The Human Resources team** at Hexagon will provide appropriate training to assist employees in complying with data protection legislation.
- 5.9 **The Head of IT** at Hexagon will hold operational responsibility for compliance with data protection legislation and best practice for information security. The organisation shall document further guidelines in the IT Security Policy.
- 5.10 **Hexagon employees** are responsible for ensuring that any personal data about them and supplied by them to Hexagon are accurate and up-to-date.
- 5.11 **Hexagon employees** are responsible for adhering to Hexagon's Data Protection policies and procedures.
- 5.12 **The Audit & Risk Committee** will review the Data Protection Policy annually and the policy will be subject to the committee's approval. The Committee will oversee internal and external data protection audit functions, review and scrutinise the Data Protection Risk Register, and exercise independent scrutiny and challenge to provide the Board with assurance.
- 5.13 **The Board** retains ultimate responsibility for Hexagon's compliance with data protection legislation and ensuring appropriate risk management arrangements are in place. The Board will review the Data Protection Policy annually and the policy will be subject to the Board's approval.

## 6 Data Protection Principles

- 6.1 Hexagon processes personal data in accordance with the principles defined in the UK GDPR and this policy is designed to ensure these principles are adhered to. Hexagon processes personal data in a fair, lawful and transparent manner.
- 6.2 **Fairness** – no data collection activities are undertaken or commissioned without an appropriate privacy notice being provided to the data subject. A privacy notice will also be supplied to the data subject whose data is being processed if personal data is being collected from sources other than the subject. All privacy information and any changes to privacy information must be guided or approved by the relevant Process Owner or the DPO. Privacy notices will be subject to yearly review.
- 6.3 **Lawfulness** – no data collection activities are undertaken or commissioned without there being a lawful ground. The Process Owner (PO) determines the lawful grounds for processing and advises on lawful processing conditions. The PO ensures there are grounds for all data processing activities that fall under their sphere of control and that the procedure for either gaining consent or establishing a legitimate interest has been followed. The lawful bases for

processing are set out in Article 6 of the UK GDPR. At least one of these must apply whenever we process personal data:

- 6.3.1 Consent: the individual has given clear consent for us to process their personal data for a specific purpose.
- 6.3.2 Contract: the processing is necessary for a contract we have with the individual, or because they have asked us to take specific steps before entering into a contract.
- 6.3.3 Legal obligation: the processing is necessary for us to comply with the law (not including contractual obligations).
- 6.3.4 Vital interests: the processing is necessary to protect someone's life.
- 6.3.5 Public task: the processing is necessary for us to perform a task in the public interest or for our official functions, and the task or function has a clear basis in law.
- 6.3.6 Legitimate interests: the processing is necessary for our legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.
- 6.3.7 If Special Category Personal Data or data relating to a criminal offence is being processed, Hexagon will establish the legal basis under Article 9 UK GDPR and Schedule One of the Data Protection Act 2018 where necessary. In addition, if Hexagon is processing personal data relating to criminal convictions and offences it shall implement suitable measures including a policy document that satisfies the requirements of the Data Protection Act 2018 Schedule 1 Parts 3 and 4.

6.4 **Transparency** – Hexagon provides sufficient information about how personal data is being processed to enable transparency about its handling. The DPO periodically reviews transparency. Data Protection policies will be reviewed yearly.

## 7 Disclosure of Data

7.1 Hexagon ensures that personal data is not disclosed to unauthorised third parties (this includes family members, friends, government bodies and in certain circumstances the police). All employees must exercise caution when

asked to disclose personal data to a third party and will receive training to deal with this risk.

- 7.2 Hexagon does not share or disclose any personal data with any other controller, organisation or individual without having first entered in a Data Sharing Agreement/Data Processing Agreement and where a legal basis has been established.
- 7.3 All requests to disclose personal data are governed by appropriate procedures and disclosures are authorised by the Head of Governance, Risk and Assurance. All data sharing activities are documented in the Register of Data Sharing Agreements and the Record of Processing Activities (ROPA).

## **8 Data Processing Purposes**

- 8.1 Data obtained for specific purposes is not used for any reason other than that purpose.
- 8.2 No data processing shall be undertaken or commissioned without the approval of the DPO who shall maintain a register of data processing activities and their purpose. Process Owners responsible for ensuring that all of the data processing activities that they undertake and/or commission have been approved by the DPO. No personal data shall be used for any purpose other than that which it was collected and/or created for without the approval of the DPO.

## **9 Data Minimisation**

- 9.1 Hexagon uses a minimum of personal data in its processing activities and periodically reviews the relevancy of the information that it collects. Process Owners ensure that no unnecessary, irrelevant or unjustifiable personal data are collected or created (directly or indirectly) through the data processing activities they are responsible for. This is recorded and monitored in the ROPA. The DPO advises on justifiable data held.
- 9.2 Use of the ROPA ensures that Hexagon does not collect information that is not strictly necessary for the purpose it was obtained.
- 9.3 All data collections forms include a fair processing statement or link to privacy information and are guided and approved by the DPO.
- 9.4 On an annual basis, all data collection methods are reviewed by the Data Protection Working Group, to ensure that personal data collected continues to be adequate, relevant and not excessive. The DPO will conduct periodic spot checks.

## 10 Data Quality

- 10.1 Hexagon recognises that the accuracy of data is important, and that some data is more important to keep up-to-date than others. Hexagon will take reasonable steps to ensure information is as accurate and current as possible (particularly where out of date or inaccurate data will have a detrimental impact on data subjects). Process Owners will ensure that personal data created either directly or indirectly through their processing activities are accurate and up-to-date. Any data that cannot reasonably be assumed to be accurate should either be erased or anonymised. The DPO can advise on data accuracy.
- 10.2 Personal data is maintained, accurate and up-to-date with every effort made to erase or rectify obsolete personal data without delay.
- 10.3 Personal data stored by Hexagon is reviewed and updated, as necessary. No data is kept unless it is reasonable to assume it is accurate.
- 10.4 The DPO and Process Owners ensure that all employees are trained in the importance of collecting accurate data and maintaining it.
- 10.5 Data subjects are expected to ensure that their personal data, held by Hexagon, is accurate and up-to-date. Completion of a registration or application form by a data subject includes a statement that the data contained therein is accurate at the date of submission.
- 10.6 Residents, customers, suppliers, employees and others are expected to notify Hexagon of any changes in circumstance to enable personal data to be updated accordingly. Hexagon will ensure any notification received regarding changes to personal data is recorded and actioned.
- 10.7 The DPO, with the collaboration of the Policy Officer, ensures that policies and procedures regarding information governance are in place and reviewed annually.
- 10.8 Each Process Owner will respond to requests for rectification from data subjects within one calendar month. This can be extended to a further two months for complex requests. If Hexagon decides not to comply with the request, the relevant Process Owner will respond to the subject to explain the reasoning and inform the subject of their right to complain to the supervisory authority and seek judicial remedy.
- 10.9 The Process Owner makes appropriate arrangements to inform processors or controllers if they have been supplied with incorrect or out-of-date personal data. They will be told the inaccurate data is not to be used and any corrections will be supplied where possible.

## **11 Data Retention**

- 11.1 In accordance with the principles of UK GDPR, Hexagon ensures that it does not retain personal data for any longer that is necessary for the purposes for which it was collected. Appropriate measures, such as erasure or anonymisation, will be applied when the data is at the end of its useful life.
- 11.2 Hexagon has a Data Retention Policy in place with the details of our data retention arrangements.
- 11.3 The DPO maintains a schedule of data retention periods in the Data Retention Schedule which defines approved retention periods and end of life treatment.

## **12 Information Security**

- 12.1 Hexagon ensures the appropriate security for any personal data that it processes (or commissions the processing of). This means taking appropriate technical or organisational measures to protect against threats including unauthorised or unlawful processing, accidental loss, destruction or damage. The Head of IT, with advice from the DPO as necessary, will ensure an IT Security Policy is maintained which sets out how data will be maintained securely, confidentially and in a way that is available.
- 12.2 Data Protection Impact Assessments are conducted as appropriate, taking into account all the circumstances of Hexagon's controlling or processing operations.
- 12.3 In determining appropriateness, the Process Owner considers the extent of possible damage or loss that be caused to the data subjects if a personal data breach a breach of security or control leading to the accidental, or unlawful, destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed occurs the effect of a breach on Hexagon, and any likely reputational damage (including the possible loss of customer trust).
- 12.4 Information security controls are selected based on identified risks to personal data, and the potential for damage or distress to data subjects whose data is being processes (as documented in the Data Protection Risk Register).
- 12.5 Hexagon complies with the data protection principles by implementing data protection policies, adhering to codes of conduct, implementing technical and organisational measures, as well as adopting techniques such as data protection by design, a Data Protection Impact Assessment Procedure, a Data Protection Breach Procedure and incident response plans.

- 12.6 All employees ensure that any personal data that Hexagon holds, and for which they are responsible, is kept securely and is not under any condition disclosed to any third party without specific authorisation by the DPO and a data sharing agreement.
- 12.7 All personal data is accessible only to those who need to use it. Where personal data is stored in a database system, only staff who need to use it have access to that system. All personal data is treated with the highest security and is kept:
- In a lockable room with controlled access; and/ or
  - In a locked drawer or filing cabinet;
  - If digital, password protected;
- 12.8 Care is taken to ensure that Personal Computer screens are not visible except to authorised employees of Hexagon. All employees enter into an Acceptable Use Agreement before they are given access to organisational information of any sort.
- 12.9 Paper records are not left where they can be accessed by unauthorised personnel and are not removed from any working environment without authorisation by their line manager. As soon as paper records are no longer required for the defined purposes, they are removed from secure archiving.
- 12.10 Personal data is deleted or disposed of in the office in line with agreed schedules and this policy. Paper records that have reached their retention date are shredded and disposed of as 'confidential waste'. Hard drives of redundant PCs are removed and destroyed before disposal.

## **13 CCTV Policy**

- 13.1 Hexagon will use CCTV to prevent and detect anti-social behaviour, prevent and detect tenancy fraud and property damage, provide safety mitigations, and crime prevention in and around some of our properties which we own or manage, our offices, car parks and communal areas where there is an assessed risk, and to help safeguard residents, colleagues and visitors to those properties and on our land.
- 13.2 Any CCTV we use, or used on our property, will be subject to a Data Protection Impact Assessment. This will be used in determining whether to either install or continue using CCTV in a specific area.
- 13.3 Hexagon will adhere to its CCTV and Audio Recording Policy to ensure that CCTV is used transparently, proportionately and compliantly to achieve the objectives identified above. The policy will ensure CCTV is routinely monitored,

fulfilling a legitimate purpose, visible, well signed, and set up to minimise unnecessary data recording.

## **14 Data Subjects' Rights**

14.1 Hexagon recognises the legal rights of the data subjects whose personal data it is processing (or intends to process) and ensures that appropriate information is provided to advise them of their rights. Data subjects have the following rights regarding data processing, and the personal data that is recorded about them:

14.1.1 To make Data Subject Access Requests regarding the nature of information held about them and to whom it has been disclosed;

14.1.2 To prevent processing likely to cause damage or distress;

14.1.3 To object to processing for purposes of direct marketing;

14.1.4 To be informed about the mechanics of automated decision-making processes that will significantly affect them;

14.1.5 To not have significant decisions that will affect them taken solely by an automated process;

14.1.6 To seek compensation if they suffer damage by any contravention of the UK GDPR;

14.1.7 To take action to rectify, block, erase, or destroy inaccurate data, including the right to be forgotten;

14.1.8 To lodge a complaint with the Information Commissioners Office;

14.1.9 To have personal data provided to them in a structured, commonly used and machine-readable format, and the right to have that data transmitted to another controller;

14.1.10 To object to any automated profiling that is occurring without consent.

14.2 Data subjects may exercise their rights through any method including, but not limited to:

14.2.1 By email;

14.2.2 Over the phone;

14.2.3 In person;

14.2.4 By letter.

## **15 Consent**

15.1 Hexagon understands 'consent' to mean a specific, informed and unambiguous indication of the data subject's wishes, given explicitly and freely. This is supplied by clear affirmative action signifying agreement to the processing of personal data relating to the subject. Consent can be withdrawn at any time.

- 15.2 Consent means the data subject has been fully informed of the intended processing and has signified their agreement, while in a fit state of mind and without pressure being exerted upon them. Consent obtained under duress or on the basis of misleading information is not a valid basis for processing.
- 15.3 Hexagon ensures that there is active communication with the data subject to demonstrate active consent. Consent is not inferred from non-response to a communication. Hexagon demonstrates that consent was obtained for the processing operation.
- 15.4 All employees must use the approved Consent form for when obtaining and recording consent; this must be in writing in order to evidence consent. There may be limited circumstances where consent can be obtained verbally either in person or over the phone, where this is the case, employees are required to record when (time/date) and what consent was obtained for, by whom, and who was consented to discuss on behalf of the customer.
- 15.5 For special categories of personal data explicit written consent of data subjects is obtained unless an alternative lawful basis for processing exists.
- 15.6 In most instances, consent to personal data (and when appropriate, special categories of data) is obtained routinely by Hexagon using standard consent documents (e.g. when a new tenant signs a tenancy agreement or during inductions for participants on a programme). These will be refreshed when reasonable.
- 15.7 Hexagon will have a lawful basis for processing a child's personal data. Consent is one possible lawful basis for processing, but it is not the only option.
- 15.8 Where Hexagon provides online services to children we will require consent and only children aged 13 or over are able to provide their own consent. For those children under 13, we will get consent from whoever holds parental responsibility for the child.
- 15.9 Special measures will be taken by Hexagon if it processes personal data relating to children under the age of 13 including the nature of privacy information provided and approach to information rights requests. As a matter of good practice, we use DPIAs to help us assess and mitigate the risks to children.

## **16 Data Transfers and Sharing**

- 16.1 Data sharing can take the form of:
- 16.1.1 A reciprocal exchange of data;

- 16.1.2 One or more controllers providing data to a third party or parties e.g. sharing CCTV images to assist with a criminal investigation;
  - 16.1.3 Several organisations pooling information and making it available to each other;
  - 16.1.4 Organisations pooling information and making it available to a third party or parties (e.g. anti-money laundering authorities);
  - 16.1.5 Exceptional, one-off disclosures of data in unexpected or emergency situation.
- 16.2 When Hexagon is obliged to share personal data for legal or regulatory reasons, it still informs data subjects accordingly unless an exception applies under Data Protection Legislation. The principal method of communicating this is via the Privacy Policy. This will apply unless sharing is required by law.
- 16.3 Any systematic or routine sharing of data between Hexagon and another party on a controller-to-controller basis is defined and detailed in a Data Sharing Agreement before any data sharing commences. This will apply unless sharing is required by law.
- 16.4 Such Data Sharing Agreements articulate the roles of the data controllers and in particular avoid any circumstances where one of the parties could otherwise be construed as a processor, rather than a controller. The agreements are filed centrally and documented in the Register of Data Sharing Agreements.
- 16.5 Hexagon only enters into data sharing activities where it is proven and documented that the data sharing is fair and lawful.
- 16.6 Hexagon only shares personal data for specified, explicit and legitimate purposes and not in a manner that is incompatible with those purposes.
- 16.7 Hexagon only shares personal data that is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- 16.8 Sharing personal data with an unauthorised controller or sharing data in the absence of a valid Data Sharing Agreement is deemed to be a data breach and is investigated by the Data Protection Officer and Process Owner in accordance with the Breach Reporting Procedure.
- 16.9 Any breach of this policy is dealt with under Hexagon's disciplinary policy and if it is also a criminal offence, the matter is reported as soon as possible to the appropriate authorities.
- 16.10 When Hexagon receives a Data Subject Rights request, such as a request to correct inaccurate personal data, Hexagon informs any other controller with whom the data has been shared.

- 16.11 When sharing information with another controller, Hexagon recognises this as a risk to the rights and freedoms of data subjects and records this in the Data Protection Risk Register.
- 16.12 Exports of data from the UK are unlawful unless there is an appropriate level of protection for the fundamental rights of data subjects.
- 16.13 Hexagon will ensure that any data transfer to a country outside the UK will have the appropriate safeguards or meet the criteria for an exception set out in the UK GDPR.
- 16.14 Hexagon is legally obliged to share certain personal data for tax, criminal or other legal reasons. In these circumstances sharing information with the relevant authority is a mandatory requirement – Hexagon will cooperate fully and share the appropriate information.
- 16.15 This Policy functions in conjunction with the Data Sharing Procedure to define how and when Hexagon shares personal data with another controller.

## **17 Record of Processing Activities (ROPA)**

17.1 Hexagon maintains a Record of Processing Activities and an analysis of data flows as part of its approach to address risks and opportunities involving personal data. Hexagon's ROPA and data flow analysis determines:

- Business processes that use personal data
- Source(s) of personal data
- Frequency of use
- How the information is backed up
- Whether the information is shared
- How information is protected
- Any risks and access controls
- Processing activity
- Maintains the inventory of data categories of personal data processed
- Recipients, and potential recipients, of the personal data
- Key systems and repositories

## **18 Risk Management**

18.1 Hexagon assesses the level of risk to data subjects associated with processing their personal data. Data Protection Impact Assessments are conducted in relation to Hexagon's processing activity and for processing done on Hexagon's behalf. Hexagon manages any risks identified by the risk assessment to ensure compliance with data protection standards.

- 18.2 Where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons, Hexagon conducts a Data Protection Impact Assessment prior to processing. A single Data Protection Impact Assessment may address a set of similar processing operations with similar risks.
- 18.3 Where, as a result of a Data Protection Impact Assessment, it is clear that Hexagon is about to commence processing of personal data that could damage and/ or distress data subjects, the decision on whether Hexagon will proceed will be reviewed by the DPO, Process Owner and Head of Governance, Risk and Assurance.
- 18.4 When there are significant concerns about either potential damage or distress, or the quantity of data concerned, the DPO will escalate to the supervisory authority.
- 18.5 Appropriate controls are selected and applied to reduce the level of risk associated with processing individual data to an acceptable level, by reference to Hexagon's documented risk acceptance criteria and the requirements of the UK GDPR. This is recorded in the Data Protection Risk Register.
- 18.6 The PO's are responsible for ensuring that all actions identified during a risk assessment or DPIA are actioned accordingly and appropriately.
- 18.7 All employees are required to undertake a risk assessment during the project planning stage and prior to changes in data processing operations or introduction of new technologies or new projects. The DPIA screening questions will support employees with establishing whether a full DPIA is required.

## **19 Personal Data Breaches**

- 19.1 Hexagon will maintain a Data Protection Incident Reporting and Recording Procedure and will ensure that all employees and those with access to personal data are aware of it.
- 19.2 The Head of Governance, Risk and Assurance shall be responsible for maintaining the Data Protection Incident Reporting and Recording Procedure and for ensuring that all relevant people are made aware of it.

## **20 Data Processors**

- 20.1 Hexagon reserves the right to contract out data processing activities or operations involving the processing of personal data in the interests of business efficiency and effectiveness, ensuring that:

- 20.1.1 There are satisfactory assurances that the processor will handle personal data in accordance with Data Protection Legislation.
- 20.1.2 Appropriate due diligence is undertaken on the proposed data processor in the field of information governance and data protection compliance prior to their appointment.
- 20.1.3 A written agreement shall be implemented between the organisation and the data processor which at least meets the requirements of the Data Protection Legislation. The data processor agreement will specify what is to happen to personal data upon termination of the data processing agreement.
- 20.1.4 No employee is permitted to commission or appoint a third party to process data on behalf of Hexagon without adhering to this policy.
- 20.1.5 The DPO shall maintain operational instructions on the steps to take to appoint a data processor. Please see the Data Sharing Procedure.

## **21 Internationalisation of personal data**

- 21.1 Hexagon will neither transfer nor process nor will it permit personal data to be transferred or processed outside the United Kingdom without the conditions laid down in the Data Protection Legislation being met to ensure that the level of protection of personal data are not undermined. Any transfer or processing of personal data that the organisation undertakes or commissions whether directly or indirectly must be approved by the DPO and may only take place if one of the following is satisfied:
  - 21.1.1 The territory into which the data are being transferred is one approved by the UK Government;
  - 21.1.2 The territory into which the data are being transferred is within the European Economic Area;
  - 21.1.3 The territory into which the data are being transferred has a decision with regard the adequacy of its data protection regime (Adequacy Regulations) issued by the UK Government;
  - 21.1.4 The transfer is made under the unaltered terms of an International Data Transfer Agreement (“IDTA”) issued by the Information Commissioner’s Office (ICO) for such purposes and where required a Transfer Risk Assessment (“TRA”) issued by the ICO for such purposes;
  - 21.1.5 The transfer is made under the provision of binding corporate rules which have been approved and certified by the UK Government;
  - 21.1.6 The transfer is made in accordance with one of the exceptions set out in the Data Protection Legislation.

21.2 Where necessary the DPO shall ensure that a risk assessment is carried out on any third country the organisation intends to transfer personal data to and that any supplementary measures are implemented as necessary to ensure adequate protection of personal data.

## **22 Training and awareness**

22.1 Hexagon will ensure that all those who it engages to process personal data either directly or indirectly are provided with appropriate training in the application of this and other data protection policies and procedures and in their data protection responsibilities.

22.2 Hexagon will also undertake data protection awareness raising activities from time to time to keep data protection front of mind. All training and awareness raising activities will be logged. Refresher training will be provided periodically.

22.3 Process Owners shall determine the training needs of those people within their sphere of control and that appropriate data protection awareness and training is provided, measured and reported.

22.4 The Head of Governance, Risk and Assurance shall implement measures to ensure that this policy is complied with.

## **23 Continuous Improvement, audit and compliance checking**

23.1 Hexagon will strive to foster a culture of data protection by design and by default in all of its data processing activities. We will ensure that measures are in place to encourage all those involved in data processing activities to adopt a model of continuous improvement to the technical and organisational measures that implement the data protection principles and safeguards into processing activities.

23.2 Hexagon will undertake periodic compliance checks to test whether its policies and procedures are being adhered to and to test the effectiveness of its control measures. Corrective action will be required where non-conformance is found.

23.3 Records will be kept of all such audits and compliance checks including corrective action requests raised.

23.4 Disciplinary action will be taken against individuals who fail to act upon the reasonable corrective action requests properly formulated and raised through data protection audits.

23.5 The Board will be provided with a summary of audit findings periodically. All data breach incidents and near misses will be reported to the Audit and Risk Committee.

- 23.6 Data compliance, collection methods, retention periods and impact assessments will be continuously reviewed by the DPO.
- 23.7 Hexagon's Data Protection Working Group will periodically review these themes. The group will be comprised of representatives from different areas of the business with the specific purpose of reviewing data protection issues.
- 23.8 This policy will be reviewed periodically and in light of any changes to our processes.

## **24 Relevant Legislation and Guidance**

- 24.1 Data Protection Act 2018 (DPA 2018)
- 24.2 UK General Data Protection Regulation (UK GDPR).

## **25 Related Hexagon policies and procedures**

- 25.1 Data Protection Incident Reporting and Recording Procedure
- 25.2 Data Subject Rights Procedure
- 25.3 Data Privacy Impact Assessment procedure
- 25.4 Data Sharing Procedure
- 25.5 Data Retention Procedure
- 25.6 ROPA Procedure
- 25.7 Data Processors Procedure
- 25.8 CCTV Policy
- 25.9 Data Retention Policy
- 25.10 Privacy Policy
- 25.11 Policy on recordings by residents
- 25.12 Cookie Policy
- 25.13 IT Security Policy
- 25.14 Employee Privacy Policy