GDPR Policy

Version Number: 2
Document Number: HAG001
Date: 01.01.20

Contents

**Henry Adams companies covered by this policy:*

Henry Adams LLP
Henry Adams Fine Art Ltd
Henry Adams Lettings (Holdings) Ltd
Gibson Gammon Residential Lettings Ltd
Henry Adams HRR Ltd
MBT Asset Management Ltd
Simply New Homes Ltd
Jacobs and Hunt Management Services Ltd
Henry Adams Ltd
Henry Adams Strategic Land Ltd
Henry Adams Lettings Ltd
Henry Adams Midhurst
Henry Adams Horsham Lettings LLP
Simply Henry Adams Ltd
Henry Adams Holiday Cottages Ltd

1.0 Introduction and background

The purpose of this policy is to outline how Henry Adams* has established measures to maintain compliance with the EU General Data Protection Regulation. The policy contains two components:

Section 2.0 – measures to re-enforce accountability and governance measures
Section 3.0 – measures to demonstrate the protection of information rights of the data subject

Approved by the Partners and Directors of Henry Adams.

1.1 Principles

Article 5 of the GDPR requires that personal data shall be:

> "a) processed lawfully, fairly and in a transparent manner in relation to individuals;
>
> b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
>
> c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
>
> d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
>
> e) 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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
>
> f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

In addition, there is a requirement that:

> "the controller shall be responsible for, and be able to demonstrate, compliance with the principles."

2.0 Accountability and governance

This policy outlines comprehensive but proportionate governance measures designed to achieve and maintain compliance with the General Data Protection Regulation. These measures have been designed to minimise the risk of breaches and uphold the protection of personal data.

This section on accountability and governance considers:

- Roles and responsibilities – the responsibilities of the Board, Data Protection Officers, information owners and general employees.
- Documentation – Henry Adams's requirements in respect of documenting processing.
- Data protection by design and default – Henry Adams requirements for Data Protection Impact Assessments.
- Lawful basis for processing – organisation's policy on determining the basis for processing.
- Security – security policy measures designed to protect information confidentiality, integrity and availability.

- Contracts – the measures that should be in place to ensure contractual relationships maintain GDPR compliance.
- International transfer – oversight measures for international transfer of data.
- Data breaches – principles for detecting and responding to data breaches.

2.1 Roles and responsibilities

Background:
While the principles of accountability and transparency have previously been implicit requirements of data protection law, the GDPR's emphasis elevates their significance. Henry Adams is expected to put into place comprehensive but proportionate governance measures.

Policy requirements:

1 Henry Adams has defined Vicki Wright BA (Hons) MNAEA as being the 'Data Protection Officer'.
2 The DPO's responsibilities include:
   - Informing and advising the organisation and its employees about their obligations to comply with the GDPR and other data protection laws.
   - Monitoring compliance with the GDPR and other data protection laws, including managing internal data protection activities; advise on data protection impact assessments; train staff and conduct internal audits.
   - Acting as the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc).
3 The DPO reports to the Management Board on a quarterly basis.
4 All information is owned by Henry Adams.
5 Board or Committee responsibility, relevant to the client – Henry Adams Management Board.

2.2 Documentation

Background:
The GDPR contains explicit provisions about documenting Henry Adams's processing activities. Henry Adams must maintain records on several things such as processing purposes, data sharing and retention. Henry Adams may be required to make the records available to the Information Commissioner's Office (ICO) on request.

Policy requirements:

6 Where Henry Adams is a controller for personal data, Henry Adams maintains documentation in a manner consistent with Article 30(1) of the GDPR.
7 Where Henry Adams is processor for personal data, Henry Adams maintains documentation in a manner consistent with Article 30(2) of the GDPR.
8 If Henry Adams processes special category or criminal conviction and offence data, Henry Adams documents:
   - the condition for processing under the Data Protection Bill;
   - the lawful basis for processing; and
   - whether the personal data is erased and retained in accordance with Henry Adams policy.
9 Henry Adams conducts regular reviews of the personal data processed and updates documentation accordingly.

2.3 Data protection by design and default

Background:
Under the GDPR, Henry Adams has a general obligation to implement technical and organisation measures to show that Henry Adams has considered and integrated data protection into processing activities.

Policy requirements:

10 Henry Adams carries out a Data Protection Impact Assessment ('DPIA') when:
   - Using new technologies; and
   - The processing is likely to result in a high risk to the rights and freedoms of individuals.

11 Processing that is likely to result in a high risk includes (but is not limited to):
- Systematic and extensive processing activities, including profiling and where decisions that have legal effects – or similarly significant effects – on individuals.
- Large scale processing of special categories of data or personal data relating to criminal convictions or offences. This includes processing a considerable amount of personal data at regional, national or supranational level that affects a large number of individuals, and involves a high risk to rights and freedoms, eg based on the sensitivity of the processing activity.
- Large scale, systematic monitoring of public areas (CCTV).

12 The decision of whether to conduct a DPIA is supported by a documented risk assessment and is endorsed by the Data Protection Officer.

2.4 Lawful basis for processing

Background:
Under the GDPR, there are six available lawful bases for processing. Henry Adams has documented the relevant lawful basis for processing and the purpose of that processing in its Information Asset Register. The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever Henry Adams processes personal data:

(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.
(b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).
(d) Vital interests: the processing is necessary to protect someone's life.
(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
(f) Legitimate interests: the processing is necessary for your 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. (This cannot apply if you are a public authority processing data to perform your official tasks.)

Policy requirements:

13 The lawful basis for processing must be considered and documented in line with the 'Documentation' section of this policy.
14 With new systems or processes, Henry Adams must determine the lawful basis and purpose of processing before beginning processing (usually as a part of the DPIA).
15 The Henry Adams public privacy notice includes the lawful basis for processing as well as the purposes of the processing.
16 If Henry Adams is processing special category or criminal offence data, both a lawful basis for processing and a special category condition for processing must be documented in the Information Asset Register and DPIA. Henry Adams should document both the lawful basis for processing and the special category condition to demonstrate compliance and accountability.

2.5 Security

Background:
The GDPR requires personal data to be processed in a manner that ensures its security. This includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage. It requires that appropriate technical or organisational measures are used.;

Policy requirements:

17 Henry Adams has defined and implemented an information security policy and supporting management system to maintain effective and proportionate security.

2.6 Contracts

Background:
The GDPR requires diligence and clarity in entering into third party relationships. Whether Henry Adams is a processor or controller, there are mandatory requirements relating to the contracts that are in place.

Policy requirements:

18 Whenever Henry Adams acts as a controller a written contract must be in place with the processors. Standards to be applied to the contracts have been defined by the Information Commissioner's Office. (see Privacy Notice).

19 Whenever Henry Adams acts as a processor, Henry Adams must only act on the documented instructions of a controller (as specified in a valid written contract). Standards to be applied to the contracts have been defined and are documented by the Information Commissioner's Office.

20 On an annual basis, the DPO will review third party relationships to determine the risk posed by processing. This will be documented as a part of a Data Protection Impact Assessment (DPIA).

21 Based on this assessment, the DPO will determine the most appropriate means to validate that contractual obligations in relation to data processing are being adhered to.

22 The DPO will present this assessment, and the results of compliance visits, to the Board at least annually.

2.7 International transfers

Background:
The GDPR imposes restrictions on the transfer of personal data outside the European Union, to third countries or international organisations. These restrictions are in place to ensure that the level of protection of individuals afforded by the GDPR is not undermined.

Henry Adams may transfer personal data where the organisation receiving the personal data has provided adequate safeguards. Individuals' rights must be enforceable and effective legal remedies for individuals must be available following the transfer. Adequate safeguards may be provided for by:

- a legally binding agreement between public authorities or bodies;
- binding corporate rules (agreements governing transfers made between organisations within in a corporate group);
- standard data protection clauses in the form of template transfer clauses adopted by the Commission;
- standard data protection clauses in the form of template transfer clauses adopted by a supervisory authority and approved by the Commission;
- compliance with an approved code of conduct approved by a supervisory authority;
- certification under approved certification mechanism as provided for in the GDPR;
- contractual clauses agreed authorised by the competent supervisory authority; or
- provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority.

Policy requirements:

23 Requests for international transfer of data must be submitted to the DPO.

24 The DPO must record requests for international transfer received.

25 The DPO will consider the DPIA in relation to this transfer and the appropriate means of adopting safeguards.

2.8 Data breaches

Background:
A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This means that a breach is more than just losing personal data. The GDPA will introduce a duty on all organisations to report certain types of data breach to the relevant supervisory authority. In some cases, organisations will also have to report certain types of data breach to the individuals affected.

Policy requirements:

26 The DPO must be notified of all breaches to this policy as soon as possible.

27 The DPO must record breaches and work with the information owner to consider the likely impact of the breach.

28 Where a breach is considered notifiable to the Information Commissioner, the DPO must immediately inform the Board.

29 A notifiable breach has to be reported by the DPO to the relevant supervisory authority within 72 hours of Henry Adams becoming aware of it. The notification must contain:

- The nature of the personal data breach including, where possible:
- The categories and approximate number of individuals concerned; and
- The categories and approximate number of personal data records concerned.
- The name and contact details of the data protection or other contact point for more information.
- A description of the likely consequences of the personal data breach.
- A description of the measures taken, or proposed to be taken, to deal with the personal data breach and, where appropriate, of the measures taken to mitigate any possible adverse effects.

30 Where a breach is likely to result in a high risk to the rights and freedoms of individuals, Henry Adams will notify those concerned directly.

31 The DPO must present an analysis of breaches and near misses to the board at least annually.

32 All employees must be trained to recognise, and escalate breaches.

2.9 Compliance and reporting

Background:
Monitoring compliance with the GDPR is a key role of the Data Protection Officer ('DPO'). The DPO must also report compliance to the Board.

Policy requirements:

33 The DPO is responsible for developing a compliance monitoring plan for this policy.

34 The compliance monitoring plan should be submitted to the Board for approval at least annually.

35 Progress to deliver the plan, exceptions noted, breaches and near misses and updates on progress to address material deviations from compliance with the policy must be reported by the DPO to the Board at least quarterly.

2.10 Training and awareness

Background:
Employee awareness of the GDPR, and their role to protect the privacy of data subjects, is core to Henry Adams's compliance programme.

Policy requirements:

36 Employees must be trained on the requirements of this policy at least annually.

3.0 Individual rights

The GDPR provides the following rights for individuals:

- The right to be informed
- The right of access
- The right to rectification
- The right to erase
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling

3.1 Right to be informed

Background:
The right to be informed encompasses Henry Adams's obligation to provide 'fair processing information', typically through a privacy notice.

Policy requirements:

37 Henry Adams maintains a privacy notice and publishes this publicly.

3.2 Right of access

Background:
Individuals have the right to access their personal data and supplementary information. The right of access allows individuals to be aware of and verify the lawfulness of the processing.

Under the GDPR, individuals will have the right to obtain:

- confirmation that their data is being processed;
- access to their personal data; and
- other supplementary information – this largely corresponds to the information that should be provided in a privacy notice.

Policy requirements:

38 All requests from subjects for access to their data should be submitted immediately to the DPO who must log the request and will:
- Consider whether the request is manifestly unfounded or excessive;
- Request copies of information held from information owners within Henry Adams;
- Review the information to ensure it does not impair the privacy of another data subject;
- Consider whether the request warrants a fee (if it requires a significant amount of data) and
- Respond to the original request.

39 A response to the request must be provided without delay and at the latest within one month of receipt. In the event the request is particularly complex or numerous, the period of compliance can be extended by a further two months. If this is the case, the DPO must inform the individual within one month of the receipt of the request and explain why the extension is necessary.

40 Performance against the response target of one month must be reported to the Board by the DPO at least annually.

3.3 Right to rectification

Background:
The GDPR gives individuals the right to have personal data rectified if it is inaccurate or incomplete.

Policy requirements:

41 Requests for rectification must be treated in the same way as requests for access. The following, additional, measures will apply:
- If Henry Adams has disclosed the personal data in question to third parties, the DPO must inform them of the rectification where possible.
- the DPO must also inform the individuals about the third parties to whom the data has been disclosed where appropriate.
- The information owner will be responsible for ensuring the requests for rectification are actioned on the information they are responsible for.
- the DPO will be responsible for validating whether requests for rectification have been properly addressed.

3.4 Right to erasure

Background:
The right to erasure is also known as 'the right to be forgotten'. The broad principle underpinning this right is to enable an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

The right to erasure does not provide an absolute 'right to be forgotten'. Individuals have a right to have personal data erased and to prevent processing in specific circumstances. These include:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
- When the individual withdraws consent.
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
- The personal data was unlawfully processed (ie otherwise in breach of the GDPR).
- The personal data has to be erased in order to comply with a legal obligation.
- The personal data is processed in relation to the offer of information society services to a child.

Policy requirements:

42 Henry Adams can refuse to comply with a request for erasure where the personal data is processed for the following reasons:
- To exercise the right of freedom of expression and information;
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority.
- For public health purposes in the public interest;
- Archiving purposes in the public interest, scientific research, historical research or statistical purposes; or
- The exercise or defence of legal claims.

43 Requests for erasure of data should be submitted immediately to the DPO and will follow the same principles as for right to access and right to rectification.

44 If Henry Adams has disclosed the personal data in question to third parties, the DPO must inform them about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.

3.5 Right to restrict processing

Background:
Individuals have a right to 'block' or suppress processing of personal data. When processing is restricted, Henry Adams is permitted to store the personal data, but not further process it.

Henry Adams is required to restrict the processing of personal data in the following circumstances:

- Where an individual contests the accuracy of the personal data, Henry Adams should restrict the processing until Henry Adams has verified the accuracy of the personal data.
- Where an individual has objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests), and Henry Adams considers whether its legitimate grounds override those of the individual.
- When processing is unlawful and the individual opposes erasure and requests restriction instead.
- If Henry Adams no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim.

Policy requirements:

45 Requests to restrict processing will be submitted to the DPO and will follow the same principles as for right to access and right to rectification, with the following additional requirements:
- The DPO must inform individuals when Henry Adams decides to lift a restriction on processing.

3.6 Right to data portability

Background:
The right to data portability allows individuals to obtain and re-use their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

The right to data portability applies:
- to personal data an individual has provided to a controller;
- where the processing is based on the individual's consent or for the performance of a contract; and
- when processing is carried out by automated means.

Policy requirements:

46 Requests for data under the right to data portability must be submitted to the DPO. (dataprotection@henryadams.co.uk)

47 The DPO is responsible for recording these and requesting the information from the information owner(s).

48 The DPO will also review the data to ensure the privacy of other data subjects is not adversely impacted.

49 The DPO will provide the personal data in a structured, commonly used and machine readable form, submitted using a secure transfer mechanism.

50 The information will be provided within one month of the original request.

51 Performance against this timescale must be reported by the DPO to the Board at least annually.

3.7 Right to object

Background:
Individuals have the right to object to:
- processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
- direct marketing (including profiling); and
- processing for purposes of scientific/historical research and statistics.

Policy requirements:

52 Requests that object to processing must be submitted to the DPO.

53 The DPO is responsible for recording and assessing these.

54 Where instructed by the DPO, Henry Adams must immediately stop processing the personal data unless:
- There are demonstrable and compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or
- The processing is for the establishment, exercise or defence of legal claims.

55 Henry Adams must inform individuals of their right to object "at the point of first communication" and in its privacy notice.

3.8 Rights relating to automated decision making including profiling

Background:
The GDPR has provisions on:
- automated individual decision-making (making a decision solely by automated means without any human involvement); and
- Profiling (automated processing of personal data to evaluate certain things about an individual). Profiling can be part of an automated decision-making process.

The GDPR has additional rules to protect individuals if an organisation is carrying out solely automated decision-making that has legal or similarly significant effects on them. Henry Adams can only carry out this type of decision-making where the decision is:
- necessary for the entry into or performance of a contract; or

- authorised by Union or Member state law applicable to the controller; or
- based on the individual's explicit consent.

Henry Adams must make sure that it:

- gives individuals information about the processing;
- introduces simple ways for them to request human intervention or challenge a decision;
- carries out regular checks to make sure that Henry Adams's systems are working as intended.

Policy requirements:

56 Henry Adams ensures it has a lawful basis to carry out profiling and/or automated decision-making and it documents this.

57 Henry Adams sends individuals a link to our privacy statement when we have obtained their personal data indirectly. In this communication Henry Adams explains how people can access details of the information we used to create their profile.

58 Henry Adams informs people who provide their personal data how they can object to profiling, including profiling for marketing purposes.

59 Henry Adams has procedures for customers to access the personal data input into the profiles so they can review and edit for any accuracy issues.

60 Henry Adams maintains additional checks in place for our profiling/automated decision-making systems to protect vulnerable groups (including children).

61 Henry Adams only collects the minimum amount of data needed and has a clear retention policy for the profiles we create.

62 Henry Adams carries out a DPIA to consider and address the risks before starting new automated decision-making or profiling.

63 Henry Adams uses anonymised data in its profiling activities.

64 The DPO regularly checks Henry Adams systems for accuracy and bias and feeds changes back into the design process.

END