Hanover (Scotland) Housing Association

Data Protection Policy and Procedures

Version: 1.2

Published October 2019

Document Control

File Name	Data Protection Policy
Original Author(s)	Anup Patel

Version	Date	Author(s)	Notes on Revision
1.0	15 May 2018	Anup Patel	Initial version
1.1	5 July 2018	Anup Patel	Updated
1.2	October 2019	Susan Campbell	Reviewed

Review

This policy shall be reviewed annually by the Data Protection Officer and amended as appropriate to reflect any changes to the requirements for the use of Hanover (Scotland) Housing Association's information assets or changes to Regulations for storage or processing of personal data. Amendments to the policy will be approved by the Chief Officers. The following table provides a record of these reviews:

Date	Reviewer	Approver	Actions
October 2019	Susan Campbell	Adam Currie	Reviewed

Distribution List

Name	Comment
All staff	Distribute to staff at induction and after updates
Interested parties (e.g., third party suppliers or regulators)	Only distribute with authorisation from the DPO

1 INTRODUCTION

This Data Protection Policy applies to all Hanover (Scotland) Housing Association entities which are located in the European Union (EU) and to any non-EU Hanover entities which are caught by the extra-territorial effect of the EU General Data Protection Regulation[1] (**GDPR**), because they process personal data relating to Data Subjects located in the EU. All Hanover entities shall be referred to in this Data Protection Policy as "we", "our", "us", or "Hanover".

We need to comply with our obligations under the GDPR whenever we process personal data relating to our employees, workers, contractors, tenants, website users and suppliers and any other individuals we interact with. This Data Protection Policy sets out our key obligations under the GDPR and how we will comply with them.

"Personal Data" means any information or data relating to an identified or identifiable Data Subject. This term will include any data that can be used to learn, record or decide something about a Data Subject. The definition of "Personal Data" is very wide, for example, an IP address may be Personal Data, as may aggregated data which is used to provide targeted advertising to an individual on the basis of their characteristics and/or behaviour.

The GDPR and this Data Protection Policy apply to all Personal Data which we Process regardless of the media on which that data is stored, or whether it relates to past or present employees, workers, tenants or supplier contacts, shareholders, website users or any other Data Subjects.

A failure to comply with the GDPR could result in enforcement action against Hanover, which may include substantial fines of up to €20 million, or 4% of total worldwide annual turnover (whichever is higher), significant reputational damage and potential legal claims from Data Subjects.

This Data Protection Policy applies to all Hanover Personnel ("you", "your") and it sets out what we expect from you in order for Hanover to comply with the GDPR. All Hanover Personnel play a vital role in ensuring that Hanover complies with its obligations under the GDPR. You must read and

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council

ensure that you fully understand and comply with this Data Protection Policy and all related policies whenever you process personal data on our behalf and you must attend all related training provided.

Your compliance with this Data Protection Policy and all related policies is mandatory. Any breach of this Data Protection Policy or any related policies may result in disciplinary action.

This Data Protection Policy and the related policies are for internal use only and cannot be shared with third parties, tenants or regulators without prior authorisation from our Data Protection Officer (**DPO**).

For definitions of capitalised terms used in this Data Protection Policy, please refer to the Definitions Addendum (Annex A) provided at the end of this Data Protection Policy.

2 SCOPE

We are committed to complying with our obligations under the GDPR and we recognise that the correct and lawful treatment of Personal Data will maintain confidence in our organisation and will provide for successful business operations. Responsible and secure use of Personal Data is a critical responsibility that we take seriously at all times. Compliance with this Data Protection Policy is overseen by our DPO. All directors, department heads and managers are responsible for ensuring that the Hanover Personnel that report to them comply with this Data Protection Policy and for implementing it and all related policies and relevant practices, processes, controls and training to ensure such compliance.

If you have any questions about the content or operation of this Data Protection Policy or the GDPR, or if you have any concerns that this Data Protection Policy is not being or has not been followed by Hanover Personnel, please contact the DPO.

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

- If you are unsure of the lawful basis which you are relying on to Process Personal Data (including the legitimate interests relied on by the Hanover)
- If you need to rely on Consent and/or Explicit Consent
- If you need to draft Privacy Notices

- If you are unsure about the retention period for the Personal Data being Processed
- If you are unsure about what security or other measures you need to implement to protect Personal Data
- If there has (or you suspect there has) been a Personal Data Breach
- If you are unsure on what basis to transfer or allow access to Personal Data outside the EU
- If you need any assistance dealing with any rights exercised by a Data Subject
- Whenever you identify that you need to carry out high risk Processing which is likely to require a DPIA or plan to use Personal Data for purposes other than what it was collected for
- If you plan to undertake any Automated Decision-Making
- If you need help with contracts or other assistance in relation to sharing Personal Data with third parties (including our suppliers).

3 LEGAL BASIS OF POLICY

3.1 THE GENERAL DATA PROTECTION REGULATION (GDPR)

3.1.1 The GDPR sets out the following principles in relation to the processing of personal data. "Processing" encompasses collection, management, disclosure, storage and disposal. To fall within the scope of the GDPR personal information must be intended to be stored in a system designed to facilitate its retrieval, whether paper based, electronic or otherwise:

I. Personal data shall be processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency');
II. Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ('purpose limitation');
III. Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
IV. Personal data shall be 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 ('accuracy');
V. 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 ('storage limitation');
VI. Personal data shall be 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 ('integrity and confidentiality');
VII. The controller shall be responsible for, and able to demonstrate, compliance with the aforementioned principles ('accountability').

3.1.2 The processing of information covers every action taken in connection with it:

- Receiving
- Organising
- Amending
- Using
- Disclosing
- Destroying

3.1.3 Personal data refers to information about a living individual which is held on a computer or in paper/manual records, as long as manual files are structured and data can be retrieved by reference to the individual in question.

3.1.4 Examples of information held on a computer include sources such as a word processing file or email trail, voicemail recordings, electronic diary system, photos and the memory of a mobile phone.

3.1.5 Information held manually requires a filing system that is well indexed and referenced so that a search for information is relatively easy.

3.1.6 Special categories of data, children's data, and data relating to criminal convictions and offences are particularly high risk and therefore are prohibited for processing unless certain conditions are met. The following types of personal data are categorised as "special categories of data":

- Race
- Ethnic origin
- Politics
- Religion
- Trade union membership
- Genetics
- Biometrics
- Health
- Sex life
- Sexual orientation

3.1.7 Processing of data relating to criminal convictions and data regarding Children (under the age of 16) also involves greater obligations under GDPR.

3.1.8 Consent of the individual to hold sensitive personal data on an employee's HR file must be obtained unless the information held is in compliance with the employer's legal obligation.

3.1.9 Images count as personal data. People who are liable to be photographed should be told that their picture may be used in a printed document or on a website and consent must be obtained. Requests by those concerned for the removal of such images should be respected.

3.1.10 CCTV recordings count as personal data. The Information Commissioner's CCTV Code of Practice should be followed, with particular reference to telling people that their images may be recorded and ensuring the security of data. Retention timescales will depend on the purpose for which images are being recorded but should be for the shortest practicable length of time. The Company Secretary will advise case by case on request. The code of practice forms Appendix 3 to this policy and can be found in The Hub/Library/Policies and procedures/procedures/Chief Executive/here.

3.1.11 Telephone recordings count as personal data. The information in a telephone recording may include data from which the identity of a person can be established, either on its own or in combination with other information.

3.1.12 The recording falls within the scope of the GDPR as it is stored in a system designed to facilitate its retrieval. Therefore the handling of telephone recording information should be treated in the same manner as any piece of data. The data subject must be informed of the recording and consent may be required from the data subject.

3.1.13 Information contained in a telephone recording will be captured by the operator and logged in the computerised call handling software to aid retrieval at a later date if required.

3.1.14 Members of staff wishing to use data already held, for a new purpose, should satisfy themselves that consent has been obtained from the data subject for such use.

3.1.15 Data subjects may exercise their right to the following in relation to their data, subject to certain exemptions such as that relating to the confidentiality of third party information:

- Access to personal data
- Objection to processing
- Objection to automated decision making and profiling
- Restriction of processing
- Data portability
- Data rectification
- Data erasure

3.1.16 There are certain conditions that must be satisfied for the transfer of information to countries outside of the EU. Such conditions include transfers subject to appropriate safeguards and transfers to countries that are deemed to ensure an adequate level of protection of personal data by the ICO. There are also derogations that allow transfer, such as if informed and explicit consent is obtained.

3.1.17 Those who process personal information must maintain a record of processing activities and conduct regular reviews against it to ensure it remains up to date.

3.1.18 The ICO also promulgates best practice in the processing of personal information and initiates enforcement of the legislation as it judges necessary.

3.2 THE HUMAN RIGHTS ACT 1998 (HRA)

3.2.1 The HRA (implementing Article 8 of the European Convention on Human Rights) grants individuals a right to respect for private and family life, the home and correspondence. It states that a public authority shall not interfere with this right except 'as is necessary in the interests of public safety or for the protection of the rights and freedoms of others.'

3.2.2 A 2009 Court of Appeal judgment defines RSLs as public authorities for HRA purposes. At the date of writing this decision is subject to appeal to the House of Lords. Regardless of this, however, Hanover is bound contractually to act as if a public authority for purposes of human rights law, for example in terms of housing support funding agreements with local authorities. These generally reflect provisions to this effect contained in the Scottish Government's model housing support funding agreement.

3.3 COMMON LAW

3.3.1 The common law imposes a duty of confidentiality in respect of any information, confidential in nature, which has been received on a confidential basis and unauthorised use of which would be detrimental to the person concerned. Such information need not be in written form.

4 COMMITMENTS

4.1 HANOVER WILL:

- Observe all statutory and common law requirements, and uphold expectations of ethical conduct, in relation to the use of personal data about those with whom it has dealings whether as customers, staff members or otherwise.
- Maintain procedural guidance to enable staff to implement policy requirements in respect of the processing of personal data. This will reflect statements of best practice as published by the Information Commissioner's Office and other regulatory bodies from time to time.
- In so doing, have particular regard to constraints on the processing of special categories of data in terms of the GPDR.
- Ensure all staff are knowledgeable of the GDPR and are equipped with the knowledge to conduct daily activities in line with this policy and the Regulation.
- Maintain a current, legally complete, registration with the ICO.
- Maintain arrangements for individuals to exercise their rights as outlined in Section 10.
- Identify a post holder to act as Data Protection Officer with responsibility for overseeing and monitoring Hanover's compliance with this policy

- Report significant policy breaches and remedial actions to the Committee of Management.
- Report data breaches within the required timescales to all necessary parties and keep a record of all breaches.

5 ROLES AND RESPONSIBILITIES

5.1.1 Data protection and security is not one person's job. It is the responsibility of each member of staff to understand the requirements to maintain a high level of data protection.

5.1.2 Support is provided via a learning and development training course to offer best practice advice. Staff should contact the Human Resources department for further information.

5.1.3 Actual and possible breaches of data protection should be promptly reported to the Company Secretary.

5.1.4 The Company Secretary is designated as the Data Protection Officer and will be the officer responsible for registering the Association with the Information Commissioner's Office (ICO) (registration no Z6439206), monitoring procedures and dealing with subject access requests. The registration entry is in the Hub here [Add link or URL].

5.1.5 All members of staff handling data are individually responsible for ensuring that they do so in accordance with the law. Particular care should be taken by staff when handling 'special categories' of data. An explanation of this is given in the policy.

5.1.6 All staff should ensure that they take care of all personal data they use in the line of their duties. Information should be kept in a secure place and should not be made available to those, both within and outside Hanover, who do not need to see it.

5.1.7 If a staff member is in doubt as to whether to make personal data available, they should consult their line manager or a senior colleague.

6 DISCLOSURE OF DATA

6.1.1 Unless another lawful basis for processing exists, explicit consent must be obtained from the individual when information about him or her is to be processed.

6.1.2 A data request may come from an MP, MSP or local authority member (Councillor). The processing of data requests from these elected representatives is permitted as long as the processing is:

- Carried out by an elected representative or a person acting with his/her authority;
- In connection with the discharge of their functions as such a representative;

- Carried out pursuant to a request made by the data subject to the elected representative to take action on behalf of the data subject or any other individual; and
- Necessary for the purposes of, or in connection with, the action reasonably taken by the elected representative pursuant to that request.

6.1.3 Processing of data requests should not be progressed if the elected representative is seeking information about a third party for whom he or she is not acting. Further information and guidance should be obtained from the Company Secretary.

6.1.4 The GDPR allows every individual about whom personal data is held, to have access to that data. Other rights of data subjects are: objection to processing; objection to automated decision making and profiling; restriction of processing; data portability; data rectification; data erasure.

6.1.5 All requests by data subjects, or those claiming to represent them, should be referred to the Company Secretary. Requests should be made on a form (Appendix 1) that should be issued to data subjects on request.

Commented [JG1]: Assume this is a separate form outside of this policy.

6.1.6 The Company Secretary will maintain a register of all information requests within the Hub and will verify the identity of the person requesting to see it and establish their right to do so. Information requests must be responded to within one month of receipt, except when requests are complex or numerous. In such an event, information will be provided within three months. The data subject will be notified of the extension and reasoning within one month.

6.1.7 For day to day routine data enquiries, staff must take reasonable steps and measures to identify the individual making the request to ensure that they are who they say they are and to confirm their entitlement for data to be disclosed.

6.1.8 If information about an individual reveals the identity of a third party, references to the third party must not be provided to the enquirer unless the third party has given permission for their data to be passed on.

6.1.9 A request received for information that might be considered 'commercially sensitive' or 'legally privileged', for example in relation to possible court proceedings, should be referred to the Company Secretary before any such information is made available.

6.1.10 The law allows Hanover to give Police personal data where it is for the purpose of prevention or detection of crime or apprehension of offenders. The consent of the subject is not required. Where a request is made the Police should be asked to submit their request in writing to the Company Secretary stating that the request is for this purpose.

7 HOUSEKEEPING

7.1.1 Staff should observe good practice as follows (reference should also be made to the relevant ICT policies and procedures):

- Filing: proper storage and labelling of records
- Clear desks: the less paper and fewer documents on them the better
- Security locks: lock computer screens and drawers when away from the desk
- Printers: apply 'locked print' facility to documents if sending to remote printers, i.e., do not print out confidential documents unless standing at printer to collect immediately
- Bins/bags: use the specified bins or bags to dispose of confidential or sensitive waste paper
- Emails: classify confidential emails in the subject heading, always check you are sending them to the right recipient and use encryption facilities for very sensitive messages
- Hard copy mail: mark as private and confidential and make sure the content cannot be viewed through outer envelope or window
- Faxes: do not fax highly confidential data
- Information retrieval: as far as possible access only the information you need, do not access any information unless authorised to do so
- Computers/mobile devices: use 'strong' alphanumeric passwords, which are harder to crack – never write them down or share them
- Documents on laptop screens: keep these out of the view of others so far as practicable
- USB memory sticks: only approved encrypted sticks may be used by authorised individuals
- Telephones: beware of bogus callers and never give out personal information without verification

8 CONFIDENTIAL PAPERS

8.1 GENERAL

8.1.1 Having the right information and documents at the right time is vital to delivering our services effectively. Managing data and documents correctly is a legal requirement and helps us to do our jobs. Knowing that it is being managed correctly provides confidence to those who need to provide and share information.

8.1.2 The common law imposes a duty of confidentiality in respect of any information which has been received on a confidential basis and unauthorised use of which would be detrimental to the person concerned. Such information need not be in written form.

8.1.3 A breach of confidentiality causing loss to someone can lead to civil liability for damages.

8.1.4 A breach of the General Data Protection Regulation can result in a criminal prosecution with an associated fine. Further civil action could follow if someone suffers a loss.

8.2 CUSTOMER CONFIDENTIALITY

8.2.1 Committees, most commonly the Housing and Care Services Committee, receive information about applicants for tenancies or existing residents. Sometimes the information about a potential tenant is given because of that person's relationship to an existing member of staff or member of the Committee of Management. Such papers require to be both confidential and transparent, in different respects.

8.2.2 Confidentiality of tenants should be maintained where tenancy problems, e.g., rent arrears, are under discussion. This helps to ensure that judgements made by Committee are based on the facts presented in the report and not any historical or assumed information.

8.2.3 However, where an applicant for housing is related to a member of staff, it is important that, for the process to be transparent, full details are given which identify both parties.

8.3 STAFFING MATTERS

8.3.1 Sometimes applications for employment are received from relatives of existing staff members. In these cases, transparency is required and both parties require to be named in the report.

8.3.2 If a matter relating to someone's employment is under discussion, e.g., their salary or a disciplinary matter, full details require to be given to the Committee, who may have regular or infrequent contact with the member of staff concerned and require to be aware of the circumstances.

8.4 GENERAL

8.4.1 The Data Classification Policy should be consulted for guidance on appropriate marking and handling of documents at different classification levels.

8.5 DISPOSAL OF CONFIDENTIAL PAPERS

8.5.1 Refer to Section 9.1.7 of this policy for guidance on the secure deletion of documents and media.

9 DOCUMENT RETENTION

9.1.1 Information regarding all personal data assets is to be maintained in the Information Asset Register, which must contain the information stated in Article 30 of the GDPR. These assets are to be classified into the following top-level groups: Internal HR Data, Tenant Data, Financial Data, Marketing Data and Contractor Data.

9.1.2 Article 5 (e) of the GDPR states that personal data shall be kept for no longer than is necessary for the purposes for which it is being processed. The retention obligation under the GDPR means in practice that the personal data should not be retained for longer than is necessary for the purposes it has been collected for (as notified to data subjects) unless it needs to be retained for longer (1) to satisfy a statutory retention requirement or (2) to deal with a legal claim.

9.1.3 Document retention guidance is set out in the Document Retention Periods spreadsheet [Ref]and applies to data regardless of its format. This derives from a model published by the National Housing Federation. It lists the principal documentation which housing associations should keep, together with details of statutory retention periods and recommended retention periods. The format of the table broadly follows the approach taken by the Institute of Chartered Secretaries and Administrators (ICSA) in its guidance on document retention and disposal. **It is the responsibility of each Chief Officer to ensure that records within their departments' control are managed consistently in terms of this procedure and that the disposal of documents is undertaken in a planned, consistent and secure manner.**

9.1.4 For each asset, a business role should be identified that 'owns' the asset. The information asset owner (IAO) is responsible for ensuring that the asset is correctly classified and for the day to day maintenance of applicable controls.

9.1.5 Measures must be in place to identify when a retention limit is reached, such that all applicable records can be deleted.

9.1.6 At the end of the retention period for the data, it is the responsibility of the IAO to ensure that the data is deleted or destroyed in a secure manner so that the data is completely unreadable and cannot be accessed or used for unauthorised purposes. The deletion must also apply to archived or backup copies of the data.

9.1.7 Acceptable methods for the secure deletion of data are currently:

a. Paper copies are to be destroyed by means of cross-cut shredders or in locked disposal bins provided by an authorised, specialist destruction company.
b. Electronic copies of documents are to be deleted with a secure deletion utility that ensures that the information cannot be retrieved. Standard deletion utilities that just remove the file pointer are not to be used.
c. Hard drives, removable media and any similar items must be securely erased prior to disposal or reassignment of the equipment. Accepted methods include utilities that meet the DoD 5220.22-M standard or encrypting the entire contents of the medium to at least AES-256 and irretrievably deleting the key.
d. Where equipment cannot be erased, physical destruction must be carried out by an authorised, specialist destruction company, and certificates of destruction provided.

9.1.8 The IAO must both sign off and record the deletion of data, including date (time if relevant), content of file and method of deletion or destruction.

9.1.9 IAOs may delegate routine tasks, in respect of the management of their assets or systems in which they are stored or processed.

9.1.10 All new information assets must be added to the Information Asset Register as and when they are acquired and removed from the register when that entire processing activity ceases and data is removed permanently.

9.1.11 Should there be any queries around the correct retention limit for a specific asset, these are to be raised with the Data Protection Officer.

9.1.12 Some records must be kept for periods specified by law. Hanover must comply with these requirements in order to avoid prosecution or regulatory action. Documents also need to be kept for commercial, management and evidential reasons, i.e., to prosecute or defend legal actions.

9.1.13 Most records have a finite useful life and can be disposed of when they no longer serve any purpose. The temptation is never to throw anything away. This 'safety first' approach can have a number of drawbacks:

- Keeping records forever can be illegal: the GDPR states that records that contain personal data should not be kept for longer than is necessary for the purpose for which they are held
- Physical storage space is expensive
- It becomes harder to find things as the volume of records increases

9.1.14 It is best to perform tasks associated with retention and disposal on a regular basis and to plan ahead. Staff need to identify records that Hanover needs to keep and to ensure these are kept in an appropriate manner and organised in a sensible way – [reference should be made to the Document Management Decision Flow Chart on the Hub]

10 DATA SUBJECTS' RIGHTS

10.1 TIMING

10.1.1 Hanover has a legal obligation to respond to an individual request made under the GDPR, confirming that the request has been actioned without undue delay and in any event within one month of receipt. In some cases, Hanover may be permitted to extend that time limit for a further two months, taking into account the complexity and number of requests received from the Data Subject.

10.1.2 If Hanover believes that it needs to extend the time limit for a response, it must write to the Data Subject within one month of receipt of their request, to inform them of this and give reasons for the delay. If you wish to extend the deadline for response to a request, please contact the Data Protection Officer.

10.1.3 Note that it may take a significant amount of time to respond to and to action a request and so it is important that a request is promptly identified and dealt with effectively. Failure to do to do could result in enforcement action from a Supervisory Authority.

10.2 THE RIGHTS

10.2.1 The rights which can be exercised against Hanover by an individual under the GDPR include:

- **The right of subject access** – The right to obtain information about how and why Hanover processes personal data about them and to obtain a copy of that data
- **The right to rectification** – The right to require Hanover to correct inaccuracies in the personal data held about them and/or to complete any incomplete personal data
- **The right to erasure ('right to be forgotten')** – The right to require Hanover to erase their personal data in certain circumstances
- **The right to restriction** – The right to require Hanover to restrict its processing of their personal data, under certain circumstances
- **The right to data portability** – The right to obtain a copy of their personal data in a certain format, to transmit it to another Controller or to require Hanover to transmit the data directly to the other Controller
- **The right to object** - The right to object to the processing of their personal data by Hanover under certain circumstances, such as the right to stop it processing it for the purposes of direct marketing.

10.2.2 This policy is divided into sections dealing with each of the rights set out above.

10.2.3 The GDPR also gives individuals other rights, such as the right not to be subject to a decision based solely on automated processing, but these rights are outside the scope of this policy.

10.2.4 Where Hanover has appointed a Processor (such as a service provider) to process its personal data, Hanover shall retain responsibility for dealing with individual requests relating to that personal data even if the request is received by the Processor and/or relates to personal data held by the Processor. Hanover's standard Processor Agreement imposes an obligation on the Processor to assist Hanover with responding to individual requests. Where this is in place, this obligation should be enforced where necessary, e.g., to obtain information or copies of personal data from the Processor, or to ask them to delete or to correct it.

10.3 RESPONDING TO REQUESTS

10.3.1 Hanover has a legal obligation to respond to all requests in a way that is concise, transparent, intelligible and in an easily accessible form, using clear and plain language. Where a data subject has made a request electronically, Hanover should provide its response to the request electronically, where possible, and unless otherwise requested by the data subject.

10.3.2 Hanover is not permitted to charge a fee for responding to these requests, unless it has clear grounds to assert that a request is "*manifestly unfounded or excessive, in particular because of their repetitive character*…"[2]. Where this is the case, Hanover has the option either to refuse to act on the request or to charge a reasonable fee, taking into account the administrative costs of responding.

10.3.3 If Hanover decides not to respond to a request in accordance with the GDPR, Hanover must inform the data subject of this without delay (and at the latest within one month of receipt of the request) including the reasons and must inform them that they can lodge a complaint with a Supervisory Authority or take legal action. If you are considering not responding to a request or charging for a response, please promptly contact the DPO.

[2] Article 12(5) of the GDPR

10.3.4 Where necessary (i.e., where there is any doubt as to the identity of the data subject) Hanover should verify the identity of the data subject making the request before actioning it (for example, before providing them with a copy of their data). Where possible, this should be done via Hanover's existing authentication procedures. However, if this is not possible, then Hanover should promptly (not later than 3 days after receipt of the request) request additional information to confirm their identity.

10.3.5 If you have any questions about how to recognise or deal with a request, please contact the DPO.

Commented [JG2]: Review whether this period is achievable & amend as required.

11 RIGHT OF DATA SUBJECT ACCESS

11.1 THE RIGHT FOR THE DATA SUBJECT

To require Hanover to confirm to the data subject whether or not Hanover processes personal data about them and if so, to provide them with the information set out below and to provide them with a copy of their personal data.

11.2 TIMING AND THE RESPONSE

The request must be responded to without undue delay and in any event within one month of receiving the request, (unless it is necessary to extend the deadline up to a further two months on the grounds set out in Section 10.1.1 above).

The following information must be provided in writing to the data subject:

- The purposes of the processing, i.e., why does Hanover process their personal data?
- The categories of personal data
- The recipients or categories of recipient to whom the personal data have been, or will be disclosed, including identifying whether a recipient receives personal data outside the EU
- Where possible, how long Hanover thinks it will store the personal data for, or if not, what criteria Hanover will use to determine this
- The fact that the data subject has the right to request rectification or erasure of their personal data, the restriction of its processing or to object to our processing of it
- The right to lodge a complaint with a Supervisory Authority
- Where the data has not been collected from the data subject themselves, any information Hanover has about the source of that data

- Where applicable, the existence of any automated decision-making, including profiling, which produces legal effects concerning them (or similarly significant effects) and at least meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject
- Where the personal data may be transferred to a country located outside the EU, what safeguards are in place governing this transfer

This information should be set out in a covering letter and sent together with a copy of the data subject's personal data which Hanover holds and/or which Hanover's Processors hold on Hanover's behalf. The initial copy must usually be provided free of charge, unless the circumstances in Section 10.3.2 above apply. A reasonable fee may be charged for further copies.

If the request has been made electronically, then Hanover should provide its response in electronic form, unless otherwise requested by the data subject.

11.3 REVIEW

Before providing a copy of the personal data to the data subject, Hanover needs to check through it to ensure that:

- Hanover is only providing personal data that relates to the data subject themselves and not personal data that relates to third parties. The data subject is only entitled to a copy of personal data that relates to them.
- If third party personal data cannot be separated out from the data subject's personal data, then the third party personal data is redacted.
- If this is not effective, for example, because the data subject would know the identity of the third party, even if the name is redacted, or because it would render the data subject's personal data unintelligible, then the document or correspondence containing the third party personal data should not be provided to the data subject in the response, unless Hanover has the consent of the third party to disclose it, or it is reasonable to disclose that data without their consent.

11.4 REFUSAL

If Hanover is unwilling or unable to comply with a subject access request, Hanover must inform the data subject of this without delay (and at the latest within one month of receipt of the request) including the reasons and inform them that they can lodge a complaint with a Supervisory Authority or take legal action.

11.5 AUDIT

A clear audit trail recording any decisions to withhold or provide information in response to a data subject access request or any decision not to comply with it, should be retained. A copy of the information and data provided to the data subject should be retained, together with a copy of any information/data which you decided not to provide.

12 RIGHT TO RECTIFICATION

12.1 THE RIGHT FOR THE DATA SUBJECT

To require Hanover to correct their personal data, if it is inaccurate, or to complete any incomplete personal data, including by means of providing a supplementary statement.

12.2 TIMING AND THE RESPONSE

Hanover must inform the data subject in writing, without undue delay and in any event within one month of receipt of their request (unless it is necessary to extend the deadline up to a further two months on the grounds set out in Section 10.1.1 above), that it has rectified their personal data and/or completed any incomplete data (as requested by the data subject).

If Hanover decides not to rectify or to complete the personal data, Hanover must inform the data subject of this without delay (and at the latest within one month of receipt of the request) and of the reasons for this and inform them that they can lodge a complaint with a Supervisory Authority or take legal action.

12.3 RECIPIENTS

Hanover must communicate the rectification of the personal data to each recipient to whom Hanover has disclosed the personal data, unless Hanover can prove that this would be impossible or would involve disproportionate effort. Hanover must inform the data subject about these recipients if requested.

12.4 AUDIT

A clear record of any decisions to rectify or complete personal data, or to refuse to do so, along with any recipients who have been informed, or any decision not to inform them (and the reasons) should be retained.

13 RIGHT TO ERASURE ('RIGHT TO BE FORGOTTEN')

13.1 THE RIGHT FOR THE DATA SUBJECT

To require Hanover to erase personal data about them, without undue delay where one or more of the following circumstances apply:

- Hanover no longer needs the personal data for the purposes it collected it;
- Hanover relies on the data subject's consent to process the data, but the data subject has withdrawn that consent and there is no other legal justification under the GDPR to process the data;
- Hanover relies on the legitimate interests justification to process the data but the data subject objects to the processing of their personal data, and there are no overriding legitimate grounds for the processing;
- The data subject objects to the processing of their personal data for direct marketing purposes;
- The personal data has been processed unlawfully;
- The personal data needs to be erased to comply with a legal obligation to which Hanover is subject; and/or
- The personal data has been collected in relation to the offer of information society services.

13.2 GROUNDS TO REFUSE TO COMPLY WITH A REQUEST FOR ERASURE

The right to erasure requires a balancing act, between the data subject's right to have the data erased and Hanover's right to retain it. Hanover does not need to erase the personal data under the GDPR if its retention is necessary for one or more of the following purposes:

- To exercise the right of freedom of expression and information
- For compliance with a legal obligation to which Hanover is subject
- For reasons of public interest in the area of public health
- For archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) of the GDPR, in so far as the erasure of the data is likely to render this objective impossible or seriously impair it
- For the establishment, exercise or defence of legal claims

13.3 TIMING AND THE RESPONSE

Hanover must inform the data subject in writing, without undue delay and in any event within one month of receipt of their request (unless it is necessary to extend the deadline up to a further two months on the grounds set out in Section 10.1.1 above), that it has deleted their personal data.

If Hanover decides not to delete the personal data, Hanover must inform the data subject of this without delay (and at the latest within one month of receipt of the request) and of the reasons for this and inform them that they can lodge a complaint with a Supervisory Authority or take legal action.

13.4 OTHER CONTROLLERS OF THE PERSONAL DATA

Where Hanover is obliged under the GDPR to delete personal data, and where Hanover has made the personal data public then, taking account of available technology and the costs involved, Hanover will be required to take reasonable steps, (including technical measures) to inform other Controllers who are processing the personal data, that the data subject has requested the erasure of any links to, or copy or replication of, the personal data.

13.5 RECIPIENTS

Hanover must communicate the erasure of personal data to each recipient to whom Hanover has disclosed the personal data, unless Hanover can prove that this would be impossible or would involve disproportionate effort. Hanover must inform the data subject about these recipients if requested.

13.6 AUDIT

A clear record of any decisions to erase or refuse a request to erase personal data and to inform/not to inform recipients/request other Controllers to delete personal data, should be retained, including the reasons.

14 RIGHT TO RESTRICTION

14.1 THE RIGHT FOR THE DATA SUBJECT

To require Hanover to restrict its processing of their personal data when one or more of the following grounds apply:

- The accuracy of the personal data is contested by the data subject. Where this applies, Hanover is required to restrict its processing of their data for a period enabling Hanover to verify the accuracy of the data;
- The processing of the data is unlawful, but the data subject does not want Hanover to erase the personal data, but asks Hanover to restrict its use instead;
- Hanover no longer needs the personal data for the purposes Hanover collected it, but it is required by the data subject to establish, exercise or defend legal claims; or
- The data subject has objected to the processing of their data, on the grounds set out in Section 16 below pending verification of whether Hanover has any overriding legitimate grounds to retain the data.

14.2 RESTRICTION

Where Hanover is required to restrict the processing of personal data, Hanover must only process it (except for the storage of it):

- With the data subject's consent;
- For the establishment, exercise or defence of legal claims; or
- For the protection of the rights of another person or company, or for reasons of important public interest.

14.3 TIMING AND THE RESPONSE

Hanover must inform the data subject in writing, without undue delay and in any event within one month of receipt of their request (unless it is necessary to extend the deadline up to a further two months on the grounds set out in Section 10.1.1 above), that it has restricted the use of their personal data.

If Hanover decides not to restrict use of the personal data, Hanover must inform the data subject of this without delay (and at the latest within one month of receipt of the request) including the reasons and inform them that they can lodge a complaint with a Supervisory Authority or take legal action.

14.4 RECIPIENTS

Hanover must communicate any restriction of the processing of personal data to each recipient to whom Hanover has disclosed the personal data, unless Hanover can prove that this would be

impossible or would involve disproportionate effort. Hanover must inform the data subject about these recipients if requested.

Hanover must inform the data subject in advance in writing, if a restriction is to be lifted.

14.5 AUDIT

A clear record of any decisions to restrict the use of personal data or to refuse to do so, and of any recipients informed (or which it has decided not to inform), should be retained, including the reasons.

15 RIGHT TO DATA PORTABILITY

15.1 THE RIGHT FOR THE DATA SUBJECT

To receive their personal data which they have provided to Hanover in a structured, commonly used and machine-readable format and the right to transmit the data to another Controller. This includes the right to have the personal data transmitted directly by Hanover to another Controller (where technically feasible) without hindrance.

This right only applies:

- To personal data which relates to the data subject. The right does not apply to anonymous data or data which doesn't relate to the data subject. This will not necessarily prevent Hanover from complying with a data portability request in relation to records that contain both data about the data subject and third parties, unless this would adversely affect the third parties, as explained further below.
- To personal data which has been provided to Hanover by the data subject. This is likely to be widely interpreted by the ICO to include not just personal data which was knowingly and actively provided by the data subject, such as in an online form, but also data that has been generated by the data subject's activity (such as data collected in an activity log). It will not apply to data which Hanover has created using that data, such as a user profile created by analysis of data collected.
- Where Hanover has relied on one or more of the following grounds as a justification to process the data under the GDPR:
  - The data subject's consent; or
  - a contract to which the data subject is a party; and
  - where the processing is carried out by automated means, and so the right does not cover paper records.

The right to data portability must not adversely affect the rights and freedoms of others. This is intended to avoid the retrieval and transmission of personal data relating to third parties to a new Controller, when this may adversely affect those third parties. When responding to a data portability request, Hanover must consider the effect this may have on any third parties. This may include where this will prevent the third party's access to a service or ensuring that trade secrets or intellectual property rights are not adversely affected. This should not prevent Hanover from complying with the request in its entirety but may restrict the scope of Hanover's response.

Hanover should not refuse to comply with a data portability request on the grounds that the data subject has infringed their contract with Hanover, such as where they have an outstanding debt.

15.2 TIMING AND THE RESPONSE

Hanover must provide the data subject with their personal data in a structured, commonly used and machine-readable format and/or transmit it to another Controller where requested (and write to the data subject to confirm that this has been done), without undue delay and in any event within one month of receipt of the request, (unless it is necessary to extend the deadline up to a further two months on the grounds set out in Section 10.1.1 above). Where necessary, Hanover should obtain confirmation from the data subject of their instructions, in advance of providing the data.

The data must be securely delivered to the data subject/other Controller, for example, using encryption and/or via strong authentication measures.

Hanover can provide the data via a direct transmission of the dataset (or the relevant extracts) or provide an automated tool that allows extraction of the relevant data. The format in which the data is provided should enable re-use of it by the data subject/the other Controller. For example, providing an individual with PDF versions of an email inbox is unlikely to enable it to be easily used. Instead it should be provided in a format that preserves all of the metadata to allow re-use.

Note that compliance with a data portability request does not require Hanover to delete the data.

Where Hanover is requested by the data subject to transmit the data to another Controller, this must be **"without hindrance",** which means that there should be no legal, technical or financial obstacles which prevent or slow down access, transmission or reuse of the data. For example, requesting payment for delivering the data, lack of interoperability or access to a data format, or excessive delay or complexity in retrieving the full dataset.

If Hanover decides not to comply with the request, it must inform the data subject of this without delay (and at the latest within one month of receipt of the request) including the reasons and inform them that they can lodge a complaint with a Supervisory Authority or take legal action.

15.3 AUDIT

A clear record of any decisions to provide personal data to a data subject, to transmit it to another Controller or to refuse to do so, should be kept.

16 RIGHT TO OBJECT

16.1 THE RIGHT FOR THE DATA SUBJECT

Where Hanover relies on legitimate interests as a justification under the GDPR to process personal data, the right to object to the processing of it, including profiling.

16.2 CRITERIA

Where Hanover receives an objection, Hanover must stop processing the personal data unless:

- Hanover can demonstrate compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject; or
- Hanover needs it in order to establish, exercise or defend legal claims.

16.3 TIMING AND THE RESPONSE

Hanover must inform the data subject in writing, without undue delay and in any event within one month of receipt of their request, (unless it is necessary to extend the deadline up to a further two months on the grounds set out in Section 10.1.1 above), that it has ceased to process their personal data.

If Hanover decides not to cease processing the personal data, Hanover must inform the data subject of this without delay (and at the latest within one month of receipt of the request) including the reasons and inform them that they can lodge a complaint with a Supervisory Authority or take legal action.

16.4 AUDIT

A clear record of any decisions to comply with an objection (or to refuse to do so) must be retained, including the reasons.

17 RIGHT TO OBJECT TO DIRECT MARKETING

17.1 THE RIGHT FOR THE DATA SUBJECT

To stop Hanover processing their personal data for direct marketing purposes (including any related profiling).

17.2 CRITERIA

Where Hanover receives this type of request, Hanover must stop using their personal data for direct marketing and related profiling. There are no exceptions.

All such requests should promptly to be sent to the [Comms Team].

17.3 TIMING AND THE RESPONSE

Hanover must inform the data subject in writing, without undue delay and in any event within one month of receipt of their request, (unless it is necessary to extend the deadline up to a further two months on the grounds set out in Section 10.1.1 above), that it has ceased the use of their personal data for marketing purposes.

17.4 AUDIT

A clear record of when and how Hanover stopped processing personal data for marketing/profiling should be retained, e.g., a suppression list or preference centre records.

18 CHANGES TO THIS DATA PROTECTION POLICY

We reserve the right to change this Data Protection Policy at any time without notice to you and so please check back regularly to read the latest copy of this Data Protection Policy. We will ensure that any substantive changes to this Data Protection Policy are brought to your attention. We last revised this Data Protection Policy on 15 May 2018.

This Data Protection Policy does not override any applicable national data privacy laws and regulations in countries where Hanover operates.

19 ACKNOWLEDGEMENT OF RECEIPT AND REVIEW

I, [EMPLOYEE NAME], acknowledge that on [DATE], I received and read a copy of this Data Protection Policy, dated [EDITION DATE] and I understand that I am responsible for ensuring that I fully understand and will comply with its terms. I understand that the information in this Data Protection Policy is intended to help Hanover Personnel work together effectively on assigned job responsibilities and to assist in the use and protection of Personal Data.

Signed	……
Printed Name	.....
Date	……

Annex A DEFINITIONS ADDENDUM

Term	Description
Automated Decision-Making	When a decision is made which is based solely on Automated Processing (including profiling) which produces legal effects or has a similarly significant effect on an individual. The GDPR prohibits Automated Decision-Making unless certain conditions are met.
Hanover Personnel	All of Hanover's employees, contractors, consultants, directors and other officers, members and others.
Consent	Agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signify agreement to the Processing of Personal Data relating to them.
Controller	A controller determines the purposes and the means of the Processing of personal data. It has the power to make high-level decisions about how and why the personal data can be used. It determines matters such as, the content of the data to be collected and used, who it will be collected about and when it will be disclosed and to whom.
Criminal Data	Personal Data relating to criminal convictions and offences or related security measures.
Data Subject	The identified or identifiable natural person that the personal data relates to, such as an employee, former employee, retiree, candidate, contractor, corporate contact, website visitor etc.
European Union	The member countries of the European Union are listed on this link: https://europa.eu/european-union/about-eu/countries_en
Explicit Consent	Consent which requires a very clear and specific statement (not merely action).
General Data Protection Regulation (GDPR)	The General Data Protection Regulation ((EU) 2016/679). Personal Data is subject to the legal safeguards specified in the GDPR.

Personal Data	Any information relating to an identified or identifiable individual. An identifiable individual is one who can be identified either directly from data, or indirectly, either on its own or together with other data which is in, or may come into, the Controller's possession. For example by reference to a name, identification number, location data, IP address, online identifier or to other factors such as physical or economic factors. This term will include any data that can be used to learn, record or decide something about an individual.
Personal Data Breach	Any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
Privacy Notices (also referred to as Fair Processing Notices or Privacy Policies)	Separate notices setting out information that must be provided to Data Subjects when Hanover collects information from or about them.
Processing or Process	Any operation or set of operations carried out in relation to personal data, such as collecting, storing, disclosing, amending and deleting. Processing is widely defined and will in effect cover any activity involving personal data, for example, storing CVs, updating employee, tenants or supplier records, monitoring employees' internet use or operating a CCTV system which captures Data Subjects' behaviour, etc.
Processor	A Processor merely Processes the personal data on behalf of the Controller. It is not able to make high-level decisions about how and why the data will be used.
Records of Processing Activity	A record of Hanover's processing activities, required by Article 30 of the GDPR.
Special Categories of Personal Data	Personal data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life/sexual orientation, genetic data or biometric data.