Housing Solutions

POLICY APPROVALS FRONT SHEET

Document Title	Data Protection Policy		
Reference	HS_POL_BIT_DAP_2.0	Version	1.1
Author	James O'Neill – Interim Head of Business Improvement		

Approval Pathway • please ensure full history of document journey is listed • please highlight the specific meeting for which this specific sheet is intended			
Group/ Meeting date	Board	ET – 20/03/18	SMT – 28/02/18
	SIT		
Outcome	Ratified	Approved for escalation	Amendment requested

Amendments made
<u>Draft to Version 1.0</u> The following sentence was added to 5.6.2. Additionally, no payments are taken over the phone, they are instead processed by a third party supplier. Resubmitted to: SMT via email (for information) Date: 02/03/18
<u>Version 1.1</u> Individuals' Rights added as an appendix following an internal audit recommendation. 5.4 had the following added: If the Privacy Impact Assessment identifies a data processing activity as high risk, this will be flagged to the nominated data protection representative who will make a recommendation as to whether or not the processing can begin or continue. If the recommendation is that processing should not begin or should desist then the assessment should be reviewed by an Executive Director who may elect to proceed with the processing despite the highlighted risks. 7.7 had the following added: (including the methods for verifying individuals' ages, obtaining consent from the child or parent(s)/guardian(s) where applicable for any day processing activity relating to child data subjects). Appendix 2 will need to be amended, but this consent form is currently with our solicitors who are providing updated wording. Resubmitted to: N/a – this advice was received before the policy was submitted to ET, but after it had been approved by SMT. The policy was resent to SMT for information, highlighting the updates. Date: 16/03/18
<u>Version 1.2</u> ... Resubmitted to: Date:

Data Protection Policy

Reference:	HS_POL_BIT_DAP_2.0	**Author:**	Interim Head of Business Improvement
Scope:	Housing Solutions	**Approved by:**	Executive Team
Legislation:	Data Protection Act 1998 General Data Protection Regulation (GDPR) (May 2018) Human Rights Act 1998 Freedom of Information Act 2000 Limitations Act 1980 Computer Misuse Act 1990 NHF Document Retention for Housing Associations Guidelines 2013 CCTV Code of Practice 2008 SP35 Social Media SP33 Information Security, Email and Internet	**Date of approval:**	20 March 2018
Related Policies:	Complaints Policy Whisteblowing Policy Disciplinary Policy Capability Policy Data Retention Policy	**Date of next review:**	20 March 2021

1. Policy Statement

1.1. This policy sets out Housing Solutions (HS) approach to Data Protection in relation to the current Data Protection Act 1998 (DPA) and the impending General Data Protection Regulation (GDPR, which will come into force on 25 May 2018).

1.2. HS recognises the need to process personal information legally under the principles set out by the DPR and GDPR and will comply with our legal requirements transparently. HS is registered with the Information Commissioner's Office as a Data Controller.

1.3. HS will ensure that when we collect and process personal information we will do so in a fair, relevant, secure and transparent way. Personal information will only be shared in accordance with the law and ensure that third parties appropriate standards of data protection.

2. Scope

2.1. This policy relates to the DPA, impending GDPR and HS' internal procedures for processing personal and sensitive information. The policy also outlines how individuals are able to access their personal information.

2.2. The requirements and accountabilities to comply with this policy apply to all HS staff, including (where necessary) any third parties engaged to carry out services on our behalf.

2.3. This policy will apply to:

- current and former customers;
- housing applicants;
- current and former employees (including Board Members and agency staff);
- prospective employees;
- volunteers;
- contractors and suppliers;
- complainants;
- others who may not fall into the above categories, but to whom HS provides services or contracts.

2.4. This policy applies to data held manually or within electronic systems that are deployed for the processing of personal and sensitive personal information. The policy details HS' (and its affiliates) obligations to compliance with data protection legislation to ensure that individuals' rights are upheld.

2.5. HS will take all reasonable measures and actions to meet our legal obligations in relation to data protection.

3. Definitions

3.1. Personal data refers to any information relating to a living identifiable person who can be directly or indirectly identified.

3.2. Sensitive personal data refers to data consisting of:

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- genetic data;
- biometric data;
- health information;
- data concerning an individual's sex life or sexual orientation.

3.3. A data subject is the person to whom personal data pertains (who is consequently the owner of the personal data).

3.4. Information Commissioner's Office (ICO) – are responsible for enforcing data protection legislation within the UK.

3.5. HS are the data controller responsible for personal information that we collect and process, as we determine the purpose and means of processing this personal data. HS' nominated representative is the Head of ICT and the deputy in their absence is the Business Performance Manager.

3.6. A data processor is any third party responsible for processing personal data on HS' behalf.

3.7. Line Managers are responsible for ensuring that their team are aware of this policy and receive appropriate training.

3.8. All staff (including Board Members) are responsible for following this policy when handling information on behalf of HS. Where a data protection breach is identified it should be reported immediately to the nominated representative (or their deputy in their absence).

4. Legislation

4.1. The existing data protection legislation is the DPA, however this will be superseded by the GDPR on 25 May 2018, which strengthens the rights of individuals (see Appendix 3).

4.2. It is likely that the GDPR will be superseded subsequently by the Data Protection Bill (DPB), however as the minutia of this Bill are in the process of being confirmed at the time of writing this policy, the policy will be updated accordingly once the DPB has passed into UK law.

4.3. HS understands that failing to comply with the requirements of the DPA (and subsequent GDPR) may result in:

- Enforcement measures (including fines) being issued by the ICO;
- Reputational impact and damage;
- Compensation for individuals for damages in relation to data breaches;
- Disciplinary action;
- Criminal and civil action;
- Personal accountability and liability;
- Organisational accountability and liability.

5. Information Held

5.1. HS is required to process personal information to provide services to customers and stakeholders. This processing can include (but is not limited to):

- Customer information (e.g. Name, Contact Details, Financial data);
- Prospective, Current or Former Employee information (e.g. Applicant details, contract terms, salaries);
- Information about other groups or persons (e.g. complainants).

5.2. When asked for personal information, individuals will be informed as to why the information is required and who will have access to it. This information will be relevant for the purpose for which it is being requested and will be kept securely.

5.3. HS will make all reasonable efforts to ensure that information held is accurate and kept up to date by the timely updating of records held. It will be explained to individuals that they have a duty to inform HS if their circumstances change so that we can update the information we hold.

5.4. When embarking on any new data processing activity or projects that may impact the data protection rights of individuals (e.g. installing new CCTV equipment, building new IT systems for storing or accessing personal data), HS will adopt a 'privacy by design' approach and conduct a Privacy Impact Assessment (Appendix 1). If the Privacy Impact Assessment identifies a data processing activity as high risk, this will be flagged to the nominated data protection representative who will make a recommendation as to whether or not the processing can begin or continue. If the recommendation is that processing should not begin or should desist then the assessment should be reviewed by an Executive Director who may elect to proceed with the processing despite the highlighted risks.

5.5. Employees and Job Applicants

5.5.1. Personal information relating to all employees is held by the Human Resources (HR) department. The Finance Department holds personal information relating to payroll and pensions. There are security restrictions in place to ensure that the HR and Finance departments cannot gain access to information that is not necessary for them to view.

5.5.2. Employment application forms contain a relevant privacy notice that explains how the form will be used and seeks consent from the applicant. If this information is to be disclosed to another party, consent will be sought from the individual (and an explanation provided regarding the implications of giving their consent).

5.5.3. Information relating to applications made by potential employees will be held for up to 12 months from the advertised closed date. After this period, the application forms of unsuccessful candidates will be destroyed. Anonymous information, such as equal opportunity statistics of candidates, will be retained.

5.6. Potential, Current and Former Customers and Contractors

5.6.1. Confidential information relating to potential, existing and former customers, contractors and suppliers is held on the Housing System, the main file server, email system and paper files within relevant departments.

5.6.2. The call recording system complies with the Payment Card Industry Data Security Standard (PCI DSS). Telephone recordings are securely held for

training and monitoring purposes and access to this is limited to the Customer Care Manager and Information, Communications and Technology department. Additionally, no payments are taken over the phone, they are instead processed by a third party supplier.

5.6.3. HS may use CCTV monitoring on its office premises and/or in residential areas to:

- protect the personal safety of customers, employees and visitors;
- investigate, detect and/or prevent crime.

5.6.4. HS complies with the CCTV Code of Practice 2008 issued by the ICO.

5.6.5. All customers are required to sign a Data Consent Form (Appendix 2), which will be updated ahead of the impending GDPR.

6. Disclosure of Information

6.1. HS may need to share information with other organisations. This will normally entail seeking and obtaining an individual's consent prior to the information being shared. However, there are some circumstances where consent may not be required, including (but not limited to):

- in connection with the assessment or collection of tax or duty (i.e. Council Tax);
- detecting or preventing crime;
- where disclosure is necessary to protect an individual's vital interests (e.g. in the event of an emergency);
- to comply with prevailing health and safety legislation;
- where a court orders the disclosure.

6.2. HS has information sharing protocols with a number of partner organisations including the Police and Local Authorities. This allows HS to transfer information between agencies for the benefit of individuals and communities. This information is not shared outside of the protocol group. Where reasonable, individuals will be informed that information about them will be subject to discussion at such a forum.

6.3. Under the Freedom of Information Act 2000, any information supplied by HS to a public body may be published in response to a Freedom of Information request.

6.4. Further guidance on what information a landlord can release can be found on the ICO website (www.ico.org.uk)

7. Access to Personal Data

7.1. All individuals that HS processes personal data for (and their representatives) have a right to obtain:

- confirmation that their data is being processed;
- access to their personal data; and
- other supplementary information (which largely corresponds to privacy notices provided when the information is collected).

7.2. Requests will preferably be made in writing, but verbal requests can be accepted. Those with learning disabilities can be assisted to access this service, or HS will assist their support worker in doing so.

7.3. At the time of writing this policy, HS currently charges a £10 administration fee (in line with the DPA) for access to personal data. This charge will be waived following the introduction of the GDPR on 25 May 2018.

7.4. HS will provide information without delay and within one month of receipt of a valid request.

7.5. If HS refuses a request for information individual reasons for this will be provided. Information will be provided unless requests are excessive or unreasonable.

7.6. A log of subject access requests and subsequent actions will be kept by HS.

7.7. Full details in relation to subject access requests are available in HS' Subject Access Request Procedure (including the methods for verifying individuals' ages, obtaining consent from the child or parent(s)/guardian(s) where applicable for any day processing activity relating to child data subjects).

8. Training

8.1. All HS employees will receive data protection training. Additional training for specific job roles will be provided as required. Training will be provided to all new starters and refreshed annually.

9. Complaints

9.1. Where an individual believes that HS has misused, allowed inappropriate access to, unreasonably refused access or to amend personal data, the grievance will be dealt with in accordance with HS' Complaints Policy.

10. Marketing and Promotion

10.1. HS will never share or sell individuals' data to third party organisations for the purposes of marketing or promotion. HS may contact individuals with information about services that are relevant, similar or complement existing services that we already provide. Individuals are able to opt out of any such communications by informing any member of HS staff who will then be responsible for updating the Housing System accordingly.

11. Equality & Diversity

11.1. HS recognises the needs of a diverse population and always acts within the scope of its own Equality and Diversity Policy, the Human Rights Act 1998, and Equalities Act 2010. HS works closely with its partners to ensure it has a clear understanding of its resident community with clear regularly updated service user profiles. HS will record, analyse and monitor information on ethnicity, vulnerability and disability.

12. Confidentiality

12.1. Under the DPA (and the impending GDPR) and the Human Rights Act 1998, all personal and sensitive organisational information, however received, is treated as confidential. This includes:

- anything of a personal nature that is not a matter of public record about a resident, client, applicant, staff or board member
- sensitive organisational information.

12.2. HS employees will ensure that they only involve other agencies and share information where there is a legal basis for processing the information.

13. Review

13.1. This policy will be reviewed by the Business Improvement Department annually and a formal review will take place on a 3 yearly basis or more frequently in response to changes in legislation, regulatory guidance, good practice or changes in other relevant Housing Solutions' policy.

13.2. Our performance in relation to the delivery of the services and activities set out in this policy will be monitored on an ongoing basis through our established reporting mechanisms to our Senior Management Team, Executive Team, Board and associated committees.

14. Appendices

14.1. Appendix 1 – Privacy Impact Assessment

Housing Solutions Privacy Impact Assessment (PIA) Template

This template has been produced using guidance from the Information Commissioner's Office (ICO) 'Conducting privacy impact assessments code of practice'.

Project/Activity Details

Provide a brief summary of what the project/activity is:

Screening questions (is there a need to do a PIA?)

The questions below are intended to help decide whether a PIA is necessary. Answering 'yes' to any of the questions in Table 1 is an indication that a PIA is required.

Table 1.

Question	Yes	No
Will the project involve the collection of new information about individuals?	☐	☐
Will the project compel individuals to provide information about themselves?	☐	☐
Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	☐	☐
Will information about individuals be used for a purpose it is not currently used for, or in a way it is not currently used?	☐	☐
Does the project involve using new technology that might be perceived as being privacy intrusive?	☐	☐
Will the project result in making decisions or taking action against individuals in ways that can have a significant impact on them?	☐	☐
Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be private.	☐	☐
Will the project require contacting individuals in ways that they may find intrusive?	☐	☐

If you have answered no to all of the questions in Table 1, it is unlikely that a PIA is necessary and you can cease the process at this point.

Consultation Requirements

Consultation can be used at any stage of the PIA process.

i) Explain what practical steps will be taken to ensure that privacy risks are identified and addressed? How will any required consultation be carried out? It may help to link any relevant stages in the project management process.

Step 1: Identify the need for a PIA

i) Why is there a need for a PIA (making reference to the screening questions if required)?

ii) What does the project/activity aim to achieve?

iii) What will the benefit(s) be to the organisation, individuals and to other parties?

iv) Please provide links to any project proposal documentation that may be relevant: (e.g. a business case)

Step 2: Describe the information flows

Describe the collection, use and deletion of personal data here. It may be useful to refer to a flow diagram or another way of explaining data flows. The below should state how many individuals are likely to be affected by the project/activity.

Step 3: Identify the privacy and related risks

Identify the key privacy risks and the associated compliance and corporate risks. Larger-scale PIAs might record this information on the corporate risk register.

Privacy Issue	Risk to Individuals	Compliance Risk	Associated Risk on the Corporate Risk Register (if required)

Step 4: Identify privacy solutions

Describe the actions that can be taken to reduce the risks and any future steps which will be necessary (e.g. the production of new guidance or future security testing for systems).

Risk	**Solution(s)**	**Result** (is the risk eliminated, reduced or accepted?)	**Evaluation** (is the final impact on individuals after implementing each solution a justified, compliant and proportionate response for the aims of the project/activity?)

Step 5: Sign off and record the PIA outcomes

Who has approved the privacy risks involved in the project? What solutions need to be implemented?

Risk	**Approved Solution**	**Approved by**

Step 6: Integrate the PIA outcomes back into the project plan

Who is responsible for integrating the PIA outcomes back into the project plan and updating any project management documentation? Who is responsible for implementing solutions that have been approved?

Action to be taken	**Date for completion of actions**	**Responsibility for action**

Who is the contact for any privacy concerns that may arise in the future?

Contact point for any future privacy concerns:

Date PIA completed:

Linking the PIA to the Data Protection Principles – Questions to Consider

Answering these questions during the PIA process will help you to identify where there is a risk that the project will fail to comply with the DPA or other relevant legislation, for example the Human Rights Act.

Principle 1
Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:
a) at least one of the conditions in Schedule 2 is met, and
b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

- Have you identified the purpose of the project?
- How will you tell individuals about the use of their personal data?
- Do you need to amend your privacy notices?
- Have you established which conditions for processing apply?
- If you are relying on consent to process personal data, how will this be collected and what will you do if it is withheld or withdrawn?

If your organisation is subject to the Human Rights Act, you also need to consider:

- Will your actions interfere with the right to privacy under Article 8?
- Have you identified the social need and aims of the project?
- Are your actions a proportionate response to the social need?

Principle 2
Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

- Does your project plan cover all of the purposes for processing personal data?
- Have you identified potential new purposes as the scope of the project expands?

Principle 3
Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

- Is the quality of the information good enough for the purposes it is used?
- Which personal data could you not use, without compromising the needs of the project?

Principle 4
Personal data shall be accurate and, where necessary, kept up to date.

- If you are procuring new software does it allow you to amend data when necessary?
- How are you ensuring that personal data obtained from individuals or other organisations is accurate?

Principle 5
Personal data processed for any purpose or purposes shall not be kept for longer than necessary for that purpose or those purposes.

- What retention periods are suitable for the personal data you will be processing?
- Are you procuring software that will allow you to delete information in line with your retention periods?

Principle 6
Personal data shall be processed in accordance with the rights of data subjects under this Act.

- Will the systems you are putting in place allow you to respond to subject access requests more easily?
- If the project involves marketing, have you got a procedure for individuals to opt out of their information being used for that purpose?

Principle 7
Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

- Do any new systems provide protection against the security risks you have identified?
- What training and instructions are necessary to ensure that staff know how to operate a new system securely?

Principle 8
Personal data shall not be transferred to a country or territory outside the European Economic Area (EEA) unless that country of territory ensures and adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

- Will the project require you to transfer data outside of the EEA?
- If you will be making transfers, how will you ensure that the data is adequately protected?

14.2. Appendix 2 – Data Consent Form

Data Protection Act 1998 Consent Form

Housing Solutions Limited ("we") are registered under the Data Protection Act 1998, (ACT) to hold information about you, our registration can be located on the Information Commissioner', (ICO) website Z6037328. The information we collect, hold, process share, retain and secure can include (but is not limited to) your personal data such as your name, address, contact details, in addition we hold sensitive personal data such as you, religious or beliefs, ethnic origin, a medical condition, police, sexuality are all types of sensitive personal information and any other information, that is relevant to managing your tenancy or providing you with a service, advice and support. This information can be collected through any means of contact that you have with Housing Solutions.

We will ensure all relevant and reasonable endeavours are in place to keep your personal and sensitive personal information securely.

Your National Insurance (NI) number is needed for the purpose of our housing relationship with you for:

- The collection of benefits
- Responding the government bodies for the payment of outstanding tax owed to them (i.e. council tax)
- The facilitation and support for your Universal Credit application including applying for alternative payment arrangements
- When applying for third party deductions for rent arrears or utility debts
- When applying for concessionary TV licences
- When referring customers for health services

We collect and share relevant information when engaging third party contractors (data processors) to carry out functions on our behalf and where necessary they will be supplied our customer information. We also collect and share information when carrying out our inter agency data sharing activities; this includes local authorities, the police and any other organisations with whom we work where the law allows. For example, we may share information with a local authority for the purposes of processing your Housing Benefit claim or let a utility company know who is living at the property and/or for the prevention and detection of crime. When doing so we will ensure they comply with our requirements under the ACT.

We may also use the information you provide and improve our services, to notify you about changes to our services, to undertake research (including but not limited to customer satisfaction surveys) and to report statistics to our regulators, local authorities and other government agencies. The information you provide may also be

used to provide you with information on activities and events that we are affiliated with.

The ACT provides you with the right to object to how your information is processed that is likely to cause or is causing damage or distress; prevent processing for direct marketing; object to decisions being taken by automated means. You also have the right in certain circumstances to have inaccurate information rectified, blocked, erased or destroyed, right to claim compensation through the courts and a right to see the information we hold about you.

If you wish to see this information please put your request in writing to the Business Improvement Data Controller, Housing Solutions, Crown House, Crown Square, Waldeck Road, Maidenhead, Berkshire, SL6 8BY or datacontroller@housingsolutions.co.uk by email. We are legally obliged to make this information available within 40 days of your request once we have received the request in writing, proof of identity and £10.

Should you terminate your tenancy with an outstanding rent balance and no payment arrangement in place, we may forward your details to a debt collection company or tracing agent. This information will be your name, address, contact details, current arrears, last payment made and tenancy start and end date. We will also share any forwarding address if you leave the property in debt with a utility company.

Our Data Protection Policy is available upon request and outlines our approach to data protection in full. If you require any further information on this matter please contact out Customer Contact Centre on 0800 876 6060 or email datacontroller@housingsolutions.co.uk. For independent advice please contact an appropriate agency such as the Citizens Advice Bureau on 03444 111 444 (www.citizensadvice.org.uk) or the Information Commissioners Office (www.ico.org.uk) on 0303 123 1113.

I understand why, how and when Housing Solutions will collect, use, share, retain and secure my information. I also understand it is my responsibility to keep my information accurate and up to date and to inform Housing Solutions if I do not want to be contacted for any form of marketing purposes. I understand I can go to my housing providers website (www.housingsolutions.co.uk) and keep up to date with how my information is processed by looking up their privacy statement as to how they process my information my change from time to time. Finally, I understand that any or all of the information that I have provided to Housing Solutions relating to other persons within my household may also be stored and used for the purposes stated on the previous pages.

Address ……..

Signed ……..

Printed ……..……

NI number ……..

Date ……

Incoming customer

Signed ……..

Printed ……..……

NI number ……

Date ……

Incoming customer (if joint tenancy)

Signed ……..

Printed ……..……

Date ……..

Witnessed on behalf of Housing Solutions

14.3 Appendix 3 – Individual's Rights

Individual's Rights

In addition to the 6 principles, the GDPR creates new rights for individuals and strengthens some of the rights that currently exist under the DPA. The GDPR provides the following rights for individuals:

i) The right to be informed

ii) The right of access

iii) The right to rectification

iv) The right to erasure

v) The right to restrict processing

vi) The right to data portability

vii) The right to object

viii) Rights in relation to automated decision making and profiling.

i) The right to be informed

The right to be informed encompasses Housing Solutions' obligation to provide 'fair processing information', typically through a privacy notice. It emphasises the need for transparency over how we use personal data. Table 1 below summarises the information that we are required to supply to individuals and Table 2 states when:

Table 1

What information must be supplied?	**Data obtained directly from data subject**	**Data not obtained directly from data subject**
Identity and contact details of the controller and where applicable, the controller's representative) and the data protection officer	✓	✓
Purpose of the processing and the lawful basis for the processing	✓	✓
The legitimate interests of the controller or third party, where applicable	✓	✓
Categories of personal data		✓
Any recipient or categories of recipients of the personal data	✓	✓
Details of transfers to third country and safeguards	✓	✓
Retention period or criteria used to determine the retention period	✓	✓
The existence of each of data subject's rights	✓	✓
The right to withdraw consent at any time, where relevant	✓	✓
The right to lodge a complaint with a supervisory authority	✓	✓
The source the personal data originates from and whether it came from publicly accessible sources		✓

Whether the provision of personal data part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the personal data	✓	
The existence of automated decision making, including profiling and information about how decisions are made, the significance and the consequences.	✓	✓

Table 2

	Data obtained directly from data subject	**Data not obtained directly from data subject**
When should information be provided?	At the time the data are obtained.	Within a reasonable period of having obtained the data (within one month)
		If the data is used to communicate with the individual, at the latest, when the first communication takes place; or
		If disclosure to another recipient is envisaged, at the latest, before the data is disclosed.

ii) The right of access

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).

A significant change in this area of legislation is that information must now be provided free of charge (unless a request is manifestly unfounded, excessive or particularly repetitive, in which case a 'reasonable fee' can be charged). Additionally, the timescales to supply information requested via a subject access request has reduced from 40 days to being provided "without delay" and at the latest within one month.

iii) The right of rectification

Individuals are entitled to have personal data rectified if it is inaccurate or incomplete. If Housing Solutions have disclosed the personal data in question to third parties, we must

inform them of the rectification where possible. We must also inform the individuals about the third parties to whom the data has been disclosed where appropriate.
Rectification requests must be responded to within one month, although this can be extended by two months where the request is complex.

iv) The right to erasure

Known as 'the right to be forgotten', this enables an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing, specifically:

- 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.

It is important to note that if the personal data in question has been disclosed to third parties, Housing Solutions must inform them about the erasure of the personal data (unless is it either impossible or involves disproportionate effort).
Housing Solutions can refuse to comply with a request for erasure 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.

v) The right to restrict processing

Individuals have the right to 'block' or suppress processing of personal data in the following circumstances:

- Where an individual contests the accuracy of the personal data, we should restrict the processing until we have 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 we are considering whether Housing Solutions legitimate grounds override those of the individual.

- When processing is unlawful and the individual opposes erasure and requests restriction instead.
- If we no longer need the personal data but the individual requires the data to establish, exercise or defend a legal claim.

It is important to note that if the personal data in question has been disclosed to third parties, Housing Solutions must inform them about the restriction of processing, unless it is impossible or involves disproportionate effort. The individual must be informed when if a decision is made to lift a restriction on processing.

vi) The right to data portability

Individuals have the right to obtain and reuse their personal data for their own purposes across different services. Essentially, this allows individuals 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 only 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.

Information must be provided free of charge and in a structured, machine readable, commonly used format (such as a CSV file). If the individual requests it, Housing Solutions may be required to transmit data directly to another organisation (if this is technically feasible). If the personal data concerns more than one individual, it is important to consider whether providing this information would prejudice the rights of any other individual.
As with other rights, we must respond without undue delay and within one month at the latest (although this can be extended by two months if the request is complex or if numerous requests are received at one time).

vii) The right to object

Individuals have the right to object to the following, based on "grounds relating to his or her particular situation":

- 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.

Housing Solutions must cease processing the personal data unless:

- you can demonstrate 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.

viii) Rights related to automated decision making and profiling

The GDPR provides safeguards for individuals to ensure that a potentially damaging decision is not taken without human intervention. Individuals have the right not to be subject to a decision when:

- it is based on automated processing; and

- it produces a legal effect or a similarly significant effect on the individual.

Housing Solutions must ensure that individuals are able to:

- obtain human intervention;
- express their point of view; and
- obtain an explanation of the decision and challenge it.

Specifically, automated decisions must not:

- concern a child; or
- be based on the processing of special categories of data unless:
    - we have the explicit consent of the individual; or
    - the processing is necessary for reasons of substantial public interest on the basis of EU / Member State law. This must be proportionate to the aim pursued, respect the essence of the right to data protection and provide suitable and specific measures to safeguard fundamental rights and the interests of the individual.

This right does not apply when a decision does not have a legal or similarly significant effect on someone, or if the decision:

- is necessary for entering into or performance of a contract between you and the individual;
- is authorised by law (eg for the purposes of fraud or tax evasion prevention); or
- based on explicit consent.

This right also defines how organisations' should handle profiling based on personal data, in particular personal data that is evaluated to analyse or predict indviduals':

- performance at work;
- economic situation;
- health;
- personal preferences;
- reliability;
- behaviour;
- location; or
- movements.

When processing personal data for profiling purposes, Housing Solutions must:

- Ensure processing is fair and transparent by providing meaningful information about the logic involved, as well as the significance and the envisaged consequences.
- Use appropriate mathematical or statistical procedures for the profiling.
- Implement appropriate technical and organisational measures to enable inaccuracies to be corrected and minimise the risk of errors.
- Secure personal data in a way that is proportionate to the risk to the interests and rights of the individual and prevents discriminatory effects.