DATA / GDPR BREACH POLICY

1. INTRODUCTION

1.1 Data Controllers and Data Processors are both subject to a general personal data breach notification regime. This means that Data Processors must report personal data breaches to Data Controllers and Data Controllers must log all personal data breaches in a register and check if they need to be reported to their supervisory authority (and in some cases, affected data subjects).

1.2 The Data Controllers are also required to maintain a Breach Register, which needs to be kept up to date and be accessible for audit by Committee, auditors and regulatory bodies. Each and every breach occurrence must be logged in the register.

1.3 The duty to notify the Information Commissioner's Office (ICO) of a breach arises where it is likely to result in a risk to the rights and freedoms of individuals. In the event of a breach that is likely to result in a high risk to the rights and freedoms of individuals, the data controller shall communicate details of the data breach both to the ICO and to the data subjects affected, without undue delay. This refers to breaches that are likely to have a significant detrimental effect on individuals. This will be further explored in section 7, where there is a full list of circumstances under which we will be required to provide a notification of a data breach to data subjects.

1.4 A sound understanding of this policy by the Committee, management and all employees is crucial, as non-compliance can lead to an administrative fine up to €10,000,000 or in case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

1.5 In some circumstances, a significant data breach should also be notified to the Scottish Housing Regulator - see their 'Notifiable Events' guidance for more information.

2. REGULATION & BEST PRACTICE

2.1 This Policy has been developed taking into account: the relevant law and sector best practice. The Regulation considered when drafting this Policy was the General Data Protection Regulation 2016/679.

3. REGISTRATION FOR DATA PROTECTION

3.1 All organisations that control and process data have to register with the Information Commissioner's Office (ICO). Lister has been registered as a Data Controller since 2002 with reference number Z616071X. The ICO website has more information about their role, people's rights, guidance and assistance - visit ico.org.uk
Further reading and updates can be found on the ICO website: https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/breach-notification/

3.2 There is an ICO office in Edinburgh at 45 Melville Street Edinburgh, EH3 7HL, telephone number 0303 123 1115.

4. AIMS & OBJECTIVES OF THIS POLICY

4.1 This policy aims to detail our approach to data breach notification. It is important relevant Committee, management and staff know how to deal with data breaches and when to notify the relevant authorities.

4.2 We ensure good quality training of this policy, which we see as vital for decision-making, and to allow staff to carry out their roles and responsibilities correctly.

5. WHAT CONSTITUTES A PERSONAL DATA BREACH?

5.1 One of the requirements of the GDPR is that, by using appropriate technical and organisational measures, personal data shall be processed in a manner to ensure the appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

5.2 The following is considered a data breach - this is not an exhaustive list and common sense should be used when assessing any data incident:

"Personal data breach" - a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

"*Destruction"*- this is where the data no longer exists, or no longer exists in a form that is of any use to the controller.

"Damage" - this is where personal data has been altered, corrupted, or is no longer complete.

"Loss of personal data" - this should be interpreted as the data may still exist, but the controller has lost control or access to it, or no longer has it in its possession.

"*Unauthorised or unlawful processing*" - include disclosure of personal data to (or access by) recipients who are not authorised to receive (or access) the data, or any other form of processing which violates the GDPR.

5.3 Any type of data breach should be categorised under one of the following sub-categories when reporting it to the appropriate authorities:

"*Confidentiality breach"* - where there is an unauthorised or accidental disclosure of, or access to, personal data.

"Availability breach" - where there is an accidental or unauthorised loss of access to, or destruction of, personal data.

"Integrity breach" - where there is an unauthorised or accidental alteration of personal data.

6. DATA BREACH - DATA PROCESSORS

6.1 In case of breach, Data Processors must notify the Data Controller *wi*thout undue delay after becoming aware of it. There are no listed exemptions from this in the Regulation and all such breaches will be reported.

7. DATA BREACH - DATA CONTROLLERS

7.1 In case of a breach that requires to be notified to the ICO, we will:

- Report the breach to the ICO, without undue delay; and, where feasible, do so no later than 72 hours after becoming aware of it.

- Where the breach notification was delayed by more than 72 hours, a letter of explanation of grounds of the delay will be attached.

7.2 Reporting of the breach will be done through: https://ico.org.uk/for-organisations/report-a-breach/ or via post on their current mailing address.

7.3 If the data breach contained sensitive personal information regarding of the data subject we will disclose this breach to the data subject affected, detailing the following in plain, clear language:

- The name and contact details of the Data Protection Officer or other contact point where more information can be obtained; *and*

- The likely consequences of the personal data breach; *and*

- The measures taken or proposed to be taken by us to address the personal data breach, including, where appropriate, to mitigate its possible adverse effects.

7.4 This is subject to the following exemptions:

- The breach is unlikely to result in a high risk for the rights and freedoms of data subjects;

- Appropriate technical and organisational protection were in place at the time of the incident (e.g. encrypted data); *or*

- This would trigger disproportionate efforts (instead, a public information campaign or "*similar measures"* should be relied on so that affected individuals can be effectively informed).

If any of the above exemptions apply, there we will not be required to notify the ICO. Any such breach will, however, still be noted in the breach database.

7.5 If there is any doubt as to whether any of them reasonably apply, we will always discuss the matter with the ICO when reporting the breach. The ICO ought to provide guidance in cases of uncertainty.
See also: https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/

7.6 Cross border data breach incidents will be reported to the relevant Members States Supervisory Authority. A list containing details of names and addresses of all registered Worldwide Supervisory Authorities can be found on the following page: http://ec.europa.eu/justice/data-protection/bodies/authorities/index_en.htm.

8. DOCUMENTATION REQUIREMENTS

8.1 A Breach Register will be created and regularly updated by us to document each incident. This register shall comprise of:

- The facts relating to the personal data breach; *and*
- Effects of the breach *and*
- The remedial action taken; *and*
- Any communications with the ICO and/or the data subjects

.

9. WHAT TO DO IF YOU WISH TO COMPLAIN ABOUT OUR BREACH NOTIFICATION POLICY?

9.1 If any party involved wishes to complain about our approach to breach notification they should refer to our Data Protection Officer who is responsible for overseeing this policy and, as applicable, developing related policies and guidelines. That post is held by:
RGDP, Level 2, One Edinburgh Quay, 133 Fountainbridge, Edinburgh, EH3 9QG.
0131 229 3239 or info@rgdp.co.uk

10. EQUAL OPPORTUNITIES

10.1 Lister is committed to ensuring equal opportunities and fair treatment for all people in its work. In implementing this policy, our commitment to equal opportunities and fairness will apply irrespective of factors such as gender or marital status, race, religion, colour, disability, age, sexual orientation, language or social origin, or other personal attributes.

11. REVIEW

11.1 This policy will be reviewed at least every three years.

Procedure note no:		Last reviewed:		
File reference:	Pdab/Lister HC Data breach policy	Last updated:		
Adopted:	28 January 2020	Review no:		©Lister Housing Co-operative Ltd