Abronhill Housing Association

Breach Notification Policy & Breach Register

Date Approved	Proposed Review Date
3 August 2020	3 August 2021

The information in this document is available in other languages or on tape/CD, in large print and also in Braille.
For details contact the Association on
01236 457948 or e-mail: admin@abronhillha.org.uk

Contents

INTRODUCTION

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 report personal data breaches to their supervisory authority in certain situations (and in some cases, affected data subjects).

Data Controllers are required to maintain a breach register, which needs to be kept up to date and freely accessible for audit (ICO / External Auditors / FOI (if applicable). Each and every breach occurrence MUST be logged within the breach register. Although all breaches must be recorded, the duty to notify the Information Commissioner's Office (ICO) of a breach is only applicable where it is **likely to result in a risk to the rights and freedoms of individuals**.

In the event that a breach 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.

A sound understanding of this Policy by the management and all employees is crucial, as non-compliance can lead to an administrative fine up to £8,000,000.00 or in case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

REGULATION & BEST PRACTICE

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.

REGISTRATION WITH THE ICO

All organisations that control and process data have to register with the Information Commissioner's Office (ICO). Abronhill Housing Association is registered as a Data Controller with the ICO and our registration number is **Z4852919**. 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/

AIMS & OBJECTIVES OF THIS POLICY

This Policy aims to detail our approach to data breach notification. It is important relevant governing body and staff as the executive know how to deal with data breaches and when to notify the relevant authority.
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.

WHAT CONSTITUTES A PERSONAL DATA BREACH?

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.
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;

- 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.

DATA BREACH - DATA PROCESSORS

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

DATA BREACH - DATA CONTROLLERS

In case of a breach, 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 the more than 72 hours, an enclosed letter of explanation of grounds of the delay will be attached;

Reporting of the breach will be done either by our DPO or data protection lead through: https://ico.org.uk/for-organisations/report-a-breach/ or via post on their current mailing address

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;
- 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.

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 register.

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.

DOCUMENTATION REQUIREMENTS

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;
- Effects of the breach;
- the remedial action taken;
- *and* any communications the ICO or the data subjects;

An example Data Breach Register can be seen in Appendix 1.
See also: https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/.

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

If any party involved wishes to complain about our approach to breach notification they should refer to our Director who is responsible for overseeing this Policy and, as applicable, developing related policies and guidelines. Our Director can be contact on 01236 457948 or at admin@abronhillha.org.uk

EQUAL OPPORTUNITES

We are 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.

REVIEW CYCLE

This policy will be reviewed annually (or, by 3 July 2021 date).

APPENDIX 1 DATA BREACH REGISTER (EXAMPLE)

The following is an example only. A breach database can take a different form, if the requirements outlined earlier within this document are satisfied.

It is a legal requirement to keep a record of all personal data breaches.

Data Controller	Abronhill Housing Association
DPO	David Mills, RGDP LLP

		Details of breach									Notification						Lessons Learned	
No.	Reference	Date/Time became aware of breach	How became aware of breach	Date / Time breach occurred	Date/Time DPO informed	Description of breach	Categories of data involved	No. of records involved	No. of data subjects affected	Actual or Potential Consequences of breach	Actions taken to resolve the breach or mitigate adverse affects	Notification to ICO required?	Date/Time of ICO notification	ICO Case Number	Data Subject Notification required?	Date/Time of Data Subject Notification	Reasons for Notification Decisions	Actions Required to prevent reoccurrence	Date of expected implementation

The full, working, excel spreadsheet ‘data breach register’ will be provided electronically along with this document template.