Data Breach Notification Procedure

Scope

This procedure applies in the event of a personal data breach under Article 33 of the UK General Data Protection Regulations (UK GDPR) *Notification of a personal data breach to the supervisory authority* and Article 34 *Communication of a personal data breach to the data subject*.

The UK GDPR draws a distinction between a 'data controller' and a 'data processor' to recognise that not all organisations involved in the processing of personal data have the same degree of responsibility. Each organisation must establish whether it is a data controller or a data processor for the same data processing activity, or whether it is a joint controller.

Responsibility

All those involved in processing data, whether employees, staff (temporary or permanent), contractors, or third-party users, together with our senior management team, are required to be aware of, and to follow this procedure in the event of a personal data breach.

It is the responsibility of all staff and users as outlined above, to report all breaches, suspected breaches, data security incidents, and data security breaches to Peter James, Director immediately they become apparent.

Where Peter James Limited, trading as Murdochs Estate Agents & Lettings act in the capacity of a data processor, we undertake to notify the data controller immediately we become aware of a breach, or suspected breach, of personal data. Full details of the breach will be recorded on our Internal Data Breaches Register.

Procedure

In the first instance, where a breach, or suspected breach, is identified Peter James must be notified immediately. Peter James is responsible for investigating the breach to identify:

1. How the breach occurred
2. When it happened and how long it was happening for
3. What categories of data were taken
4. The number of records/subjects affected
5. How you have mitigated the breach
6. Consequences of the breach
7. Any other information relating to the breach

It is the responsibility of all those involved in processing personal data on our behalf, to co-operate fully with any investigation in order that the full facts can be established, and reporting timeframes adhered to.

Where necessary, third parties will be engaged to assist with any investigation, for example, IT specialists, capable of forensic analysis of our IT infrastructure, to identify the cause and extent of any breach of our information security systems.

Where a breach occurs with a data processor, processing on our behalf, Peter James will liaise with the processor to conduct the necessary investigation. The responsibilities of both parties, in the event of a data breach, are clearly defined in the Data Sharing Agreement signed by both parties.

Breach Response

A personal data breach can occur in several ways including, in respect of personal data transmitted, stored, or otherwise processed:

- A breach of security leading to the accidental or unlawful destruction of data
- A breach of security leading to the accidental or unlawful access to our data by an unauthorised third party
- Loss of data
- Alteration of data
- Unauthorised disclosure

Our response to a breach will depend on the nature of the breach. However, in all cases, we must ensure that our systems and data are secured to prevent further damage.

Actions may include changing passwords or improving security such as firewalls and virus software.

Employees and third parties processing data on our behalf are encouraged to report breaches immediately, this includes where a breach has occurred due to an error of a member of staff, or someone processing data on our behalf. In the first instance, additional training will be provided. Disciplinary action will only be considered in the event of repeated breaches by an individual, or a breach caused by the willful act/negligence of an individual.

Actions within the company may need to be assessed such as email time delay, to reduce the possibility of a data breach occurring.

Notification of Breach

In every case, as the data controller, we are responsible for determining whether the breach poses a risk to the rights and freedoms of the data subjects involved.

Information Commissioner's Office

If it is determined that a risk exists, notification must be made to the ICO without undue delay but in all cases within 72 hours.

Notification to the ICO must be submitted electronically and include the results of our investigation including points 1 – 7 above.

If the investigation is on-going, we must still submit our notification within 72 hours to include all information available at that point in time. Further information can be sent in phases to the ICO, as it becomes available. This timeframe is chronological hours, not business hours. It is therefore vital that all staff respond to any breach, or suspected breach, by immediately reporting it to Peter James.

Where notification is not possible within 72 hours, a breach notification must be submitted electronically at the earliest possible opportunity, with justification for the delay.

We will always co-operate fully with the ICO, and any investigation they instigate. We agree to abide by any decision and guidance they issue.

Data Subject/s
Where the outcome of the investigation indicates a ***high*** risk to the rights and freedoms of the data subject, we must notify the data subject as soon as possible.

Notification must be made in clear and plain language, and include information outlined in points 1 – 7 above.

If the breach affects a high volume of data subjects and personal data records, we will assess the amount of effort involved in notifying each data subject individually. Where we consider that the amount of work involved would hinder our ability to provide appropriate notification to the data subjects within the specified time frame, we may use public communications or similar measures to inform those affected in an equally effective manner.

Where we have not notified the data subject, and the supervisory authority considers the breach will result in the likelihood of a high risk to the data subject, we will communicate the data breach to the data subject using the quickest and most appropriate means possible, for example, E-Mail or telephone call.

Should a data subject wish to complain about a data breach, they are entitled to do so, and we will advise them of our complaints procedure, and their right to complain to the ICO.

Once the breach has been investigated, reported where necessary and mitigating actions instigated, Peter James must ensure that full details are recorded on our internal breaches register.

This policy, and matters arising from it are reviewed annually and are the responsibility of Peter James.