# Personal Data Breach Policy

## Annex 2 – Data Breach Risk Assessment

Family Wise Ltd takes Data Breaches very seriously.

If a Data Breach has occurred a risk assessment should be made immediately and recorded on the Data Breach Incident form.

The following guidance provides a Framework for assessing whether the Information Commissioners Office or effected individuals need to be notified of the personal data breach.

### The Risk Assessment Approach

When completing the risk assessment, take into account:

- The type of breach - The nature, sensitivity, and volume of personal data.
- Ease of identification of individuals.
- Severity of consequences for individuals.
- Special characteristics of the individual.
- Existing availability of data.

There are a limited number of circumstances where, even when Family Wise Ltd is aware of a breach of personal data, there may be containment actions that will remove the need for notification to the ICO but should still need to be recorded on the Data Breach Record. Under the following circumstances notification may not be necessary;

- Encryption – where the personal data is protected by means of encryption.
- 'Trusted' partner - where the personal data is recovered from a trusted partner organisation.
- Cancelling the effect of a breach - where the Family Wise Ltd can null the effect of any personal data breach.

### Grading the Breach

Firstly, establish the likelihood that an adverse effect to individuals may occur from the personal data breach. The table below can be used as a guide.

| No. | Likelihood of adverse effect | Description |
|---|---|---|
| 1 | **Not occurred** | There is absolute certainty that there can be no adverse effect. |
| 2 | **Not likely** (or any incident involving vulnerable groups even if no adverse effect occurred) | In cases where there is no evidence that can prove that no adverse effect has occurred this must be selected. |
| 3 | **Likely** | It is likely that there will be an occurrence of an adverse effect arising from the breach. |
| 4 | **Highly likely/Occurred** | There is almost certainty that at some point in the future an adverse effect will happen or there is a reported |

| | | |
|---|---|---|
| | | occurrence of an adverse effect arising from the breach. |

Next, grade the severity of any possible adverse effect to individuals. The table below can be used as a guide.

| No. | Severity of Adverse Effects on Individuals | Description |
|---|---|---|
| **1** | **No adverse effect** | There is absolute certainty that no adverse effect can arise from the breach. |
| **2** | **Minor** | A minor effect must be selected where there is no absolute certainty. A minor adverse effect may be where there is a possible inconvenience to the individuals effected – such as temporary unavailability of a non-crucial account. |
| **3** | **Adverse** | An adverse effect may be release of confidential information into the public domain leading to embarrassment or it prevents someone from doing their job. |
| **4** | **Severe** | A severe effect may be where the breach could result in identity theft or fraud, physical harm, psychological distress, humiliation, or damage to reputation. |

Both the likelihood and adverse values form part of the Data Breach Assessment Grid.

**Data Breach Assessment Grid**

This operates on a 4x4 basis, with anything other than 'grey breaches' being reportable to the Information Commissioner's Office within 72 hours of becoming aware of the breach. 'Red breaches' require notification to individuals whose personal data has been breached.

| | | | | | | |
|---|---|---|---|---|---|---|
| **Impact** | **Serious** | **4** | 4 | 8 | 12 | 16 |
| | **Adverse** | **3** | 3 | 6 | 9 | 12 |
| | **Minor** | **2** | 2 | 4 | 6 | 8 |
| | **No Adverse Effect** | **1** | 1 | 2 | 3 | 4 |
| | | | **1** | **2** | **3** | **4** |
| | | | **Not Occurred** | **Not Likely** | **Likely** | **Highly Likely** |
| | | | **Likelihood that individuals' rights have been affected.** | | | |