Personal Data Breach Policy & Procedure

Policy:

The GDPR introduces a duty on all organisations to report ***certain types*** of personal data breach to the relevant supervisory authority (ICO for individuals in the UK). We must do this within 72 hours of becoming aware of the breach, where feasible.

Procedures:

- Keep a record of any personal data breaches, regardless of whether we are required to notify the ICO.
- When a personal data breach has occurred, we need to establish the likelihood and severity of the resulting risk to people's rights and freedoms.
- If the breach is likely to result in a **low risk** of adversely affecting individuals' rights and freedoms, we must inform both the ICO.
- If the breach is likely to result in a **high risk** of adversely affecting individuals' rights and freedoms, we must inform both the ICO **and** those individuals without undue delay.
- Ensure we have robust breach detection, investigation and internal reporting procedures in place. This will facilitate decision-making about whether or not you need to notify the relevant supervisory authority and the affected individuals.

Appendix:

All information from the ICO on Personal Data Breach Policy can be seen on following this link: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/

To notify the ICO of a personal data breach, please see our pages on reporting a breach.

Remember, in the case of a breach affecting individuals in different EU countries, the ICO may not be the lead supervisory authority. This means that as part of your breach response plan, you should establish which European data protection agency would be your lead supervisory authority for the processing activities that have been subject to the breach. For more guidance on determining who your lead authority is, please see the WP29 guidance on identifying your lead authority, which has been endorsed by the EDPB.