Template Data Breach Protocol

Q: What is a personal data breach?

A: 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 (Article 4 (12) GDPR).

Phase 1 – immediate actions (first line employee)

If you become aware of or cause a personal data breach (or if you are unsure), contact without delay the data protection officer (DPO), relevant partner or line manager in your office. Do not delay in notifying a breach.

The communication should include as much information as is available relating to the following:

- the nature of the personal data breach;
- the categories and approximate number of data subjects concerned;
- the categories and approximate number of personal data records concerned;
- whether the breach is ongoing; and
- the time and date the notifier became aware of the breach

You may not have full information before notifying the breach, however this should not delay your notification.

Phase 2 – Assessing the breach ([firm's DPO and/or relevant senior stakeholders])

- Log the breach in your breach register. Keep records of decisions taken relating to the breach and reasons why.
- Gather as much information as possible.
- In relation to the breach, find out whether you are a data controller or data processor, as this will impact your notification obligations. As an employer you will be a data controller of any personal data you hold relating to your employees. If for example you are acting for a financial institution and the breach relates to personal data of the financial institution's customers, your firm may be the data processor and your firm's obligation will be to notify your client, the financial institution, and not the data subjects. However, always check the arrangement/contract with your client.
- Take measures to address the data breach, including measures to mitigate possible adverse effects for example, if the breach was caused by sending an email and/or attachment in error, seek to get confirmation from the email recipient that they have deleted the email and/or attachment. See **Appendix 1** for sample text.
- If the issue has been caused by a third-party supplier, check your contract with them and ensure that they are complying with their contract and legal

obligations, including providing you with the necessary information, including confirmation of resolution.
- Consider the likely consequence of the breach and document them.
- Consult the firm's insurance policy and where appropriate contact the firm's insurer.

Phase 3 – Notification ([firm's DPO and/or relevant senior stakeholders])
Consider your notification obligations.

- Data Protection Commission:
    - Where required, prepare to notify the Data Protection Commission. As a data controller, you must notify without undue delay and within 72 hours of becoming aware of the breach, unless the breach is unlikely to result in a risk to the rights and freedoms of the data subject(s). Please note that the 72 hours runs over the weekend, public holidays etc, so if you become aware of a breach on a Friday at 3pm, you have until 3pm the following Monday to notify the breach. Consult Article 33 of the GDPR for further detail including the detail to be included in the notification.
- Data Subjects (employees, clients):
    - Where required (as a data controller), prepare to notify the data subjects. Data subjects must be notified without undue delay and within 72 hours of becoming aware of the breach, where the breach is likely to result in a high risk to the rights and freedoms of the data subject(s). For example, if the data is encrypted and not capable of being unencrypted and no data loss has occurred the breach is unlikely to require notification to the data subject(s). Consult Article 34 of the GDPR for further detail including the detail to be included in the notification.
- Data Controller (clients):
    - If your firm is acting as a data processor the client/data controller will need to be notified without undue delay, or as set out in contract/terms and conditions. Note that data processing contracts often contain response times that are shorter than 72 hours.
- Consider if any other party needs to be notified (Gardaí, the Law Society)?

Phase 4 ([firm's DPO and/or relevant senior stakeholders])

- Make any follow-on submissions to the Data Protection Commission and other relevant parties.
- Write up a final report on the incident.
- Ensure that the breach register is up to date and mark the matter as closed
- Ensure that all necessary correspondence is saved for future reference (notification letters, assurances from third parties, responses from clients, data subjects, Data Protection Commission).
- Identify any matters that can be improved for example, staff training, changing supplier/vendor, assessing systems/applications (including user access controls)

- Implement recommendations.

Appendix 1
Email to be sent to error recipient when firm's employee has sent email and/or attachment in error.

To be adapted as necessary

Dear [XXX],

In relation to the e-mail sent to you on the [XX/XX/XXX] at [XX:XX], this email and/or attachment was sent in error. I apologise for the inconvenience.

I would be grateful if you could please confirm by return the following:

1. That you deleted the email and/or attachment;
2. That you have not further distributed or transferred the email and/or attachment;
3. That you have not and will not use the information contained within the email and attachment for any purpose;
4. That (if necessary) we can share this confirmation with a third party ([e.g. client, data protection supervisory authority]) (redacting your personal details where possible).

Thank you very much for your assistance and I am sincerely sorry for any inconvenience caused.