

PDF Sample DATA BREACH RESPONSE AND NOTIFICATION PROCESS

1. SCOPE, PURPOSE AND **USERS**

This Procedure provides general principles and approach model to respond to, and mitigate breaches of personal data (a “personal data breach”) in one or both of the following circumstances:

- The personal data identifies data subjects who are residents of the Member States of the European Union (EU) and countries in the European Economic Area (EEA), regardless of where that data is subject to processing globally; and
- The personal data is subject to processing in the EU and/or EEA, regardless of the country of residency of the data subject.

This Procedure is applicable also for any other type of security incident.

The Procedure lays out the general principles and actions for successfully managing the response to a data breach as well as fulfilling the obligations surrounding the notification to Supervisory Authorities and individuals as required by the EU GDPR.

All Employees/Staff, contractors or temporary Employees/Staff and third parties working for or acting on behalf of **.....Ltd (“Company”)** must be aware of and follow this Procedure in the event of a personal data breach, or other security weakness or an incident.

1. Reference documents

- EU GDPR 2016/679 (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons about the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC)
- Information Security Policy
- List of Legal, Regulatory, Contractual and Other Requirements
- Personal Data Protection Policy

2. **Definitions**

The following definitions of terms used in this document are drawn from Article 4 of the European Union’s General Data Protection Regulation (GDPR):

“**Personal Data**” means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person Regulation.

“**Controller**” is the natural or legal person, public authority, agency or any other body, which alone or jointly with others, determines the purposes and means of the processing of personal data.

Commented [dk1]: Key element of the GDPR and its whole purpose which is to avoid a breach. This Policy provides the relevant guidance in how to be applicable

Commented [dk2]: Point 3 -12 are key elements and guide as to all GDPR key definitions that apply

“**Processor**” is a natural or legal person, public authority, agency or any other body which processes personal data on behalf of a Data Controller. Traceable and Accurate information that the team can rely on to assist through any Data Breach and thereby make appropriate prompt response to the relevant interested parties, e.g. Processor/Controller, Data Subject and if required the relevant Supervisory Authority

“**Processing**” means any operation or set of operations which is performed on personal data or on sets of personal data, whether by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

“**Personal Data Breach**” means 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.

“**Supervisory Authority**” means an independent public authority which is established by a Member State pursuant to Article 51.

3. Data Breach Response Team

A Data Breach Response Team must be a multi-disciplinary team comprised of knowledgeable and skilled individuals in **IT Department & Security, Legal, H.R. and Senior Management**. The team may physically respond to any suspected/alleged data breach or security weakness or incident referred to as a data breach.

Managing Director appoints the members of the Data Breach Response Team. The Team must be appointed regardless of whether a breach has occurred.

The team must ensure that necessary readiness for a data breach response exists, along with the needed resources and preparation (such as call lists, substitution of key roles, desktop exercises, plus required review of company policies, procedures and practices).

The team’s mission is to provide an immediate, effective, and skilful response to any suspected/alleged or actual data breach affecting the business.

If required, the team members may also involve external parties (e.g. an information security vendor for carrying out digital forensics tasks or an external communications agency for assisting the Company in crisis communications needs).

The Data Breach Response Team may deal with more than one suspected/alleged or actual data breach at a time.

The Data Breach Response Team must be prepared to respond to a suspected/alleged or actual data breach 24/7, year-round. Therefore, the contact details for each member of the Data Breach Response Team, including personal contact details, shall be stored in a central location, and shall be used to assemble the team whenever notification of a data breach is received.

Commented [dk3]: Traceable and Accurate information that the team can rely on to assist through any Data Breach and thereby make appropriate prompt response to the relevant interested parties, e.g. Processor/Controller, Data Subject and if required the relevant Supervisory Authority

Commented [dk4]: Guide to how to set up a GDPR R.T.