**Subject:** This document describes the procedure for reporting a personal data security breach.

**Scope:** General Data Protection Regulation.

**Normative Reference(s):** /

Table of contents :

[**I.** **Objective of the procedure** 2](#_Toc5366127)

[**II.** **The internal procedure** 2](#_Toc5366128)

1. **Objective of the procedure**

The aim of this internal document is to **define** a personal data breach in connection with a personal data processing operation.

**Definition:**

A personal data breach means the loss of availability, integrity or confidentiality of personal data, whether accidentally or unlawfully, during processing of the data by the company.

A breach of personal data due to a company's carelessness and negligence when processing such data now carries a direct and heavy penalty including criminal sanctions.

1. **The internal procedure**

**Step-by-step approach:**

* All MANE Group employees, customers, suppliers, subcontractors, service providers and other partners or contractors who become aware of a breach of the obligations arising from the European General Data Protection Regulation (GDPR) must notify directly and immediately the Group's Data Protection Officer (DPO) Julie Royo-Renaudin (SJPI) at the email address [dpo@mane.com](mailto:dpo@mane.com) or the relevant DP Coordinator who will forward the information immediately to the DPO.

Any such notifications to the DPO at the email address[dpo@mane.com](mailto:dpo@mane.com) shall at least:

* Communicate the name and contact details of the person reporting the alleged breach or those of another contact point where more information can be obtained;
* Communicate the name of the personal data processing operation concerned;
* Communicate the name of the data controller and the relevant department and entity within the Group;
* Describe the nature of the personal data breach, including the categories and approximate number of persons involved in the breach;
* Describe the likely consequences of the personal data breach;
* Describe the measures taken or that should be taken to address the personal data breach or to mitigate its adverse effects.
* The DPO shall inform the Information Systems Director (ISD) of the breach by email without delay.
* The DPO and the ISD shall convene the employees concerned for preliminary implementation of the compliance actions and a decision on what further course of action to take.

**Characterisation of the breach**

|  |  |
| --- | --- |
|  |  |
| Personal data processing operation concerned/Nature of the personal data concerned |  |
| Human or computer error |  |
| External malice |  |
| Nature of the breach (loss of availability, integrity or confidentiality) |  |
| Date and time of the breach |  |
| Use of a processor |  |

**Crisis management priority actions**

|  |  |
| --- | --- |
|  |  |
| Convening the crisis unit |  |
| Analysis of the causes and consequences of the incident |  |
| Reconstruction and remedial plan  Determining immediate technical measures |  |
| Gathering and preservation of evidence in case of an attack or malicious activity |  |
| Notification of CNIL within 72 hours maximum |  |
| Notification of the data subjects concerned |  |
| Notification of insurance |  |
| Complaint mechanisms |  |

* If the breach is confirmed, the DPO will inform the CNIL and the data subjects concerned.

The MANE Group's DPO shall take all the necessary measures to notify the breach in question to the supervisory authority (CNIL) not later than 72 hours after having become aware of it, unless the breach is unlikely to result in a risk to the rights and freedoms of the natural persons concerned.

The CNIL has supervisory powers and the convictions handed down by it may be published on its website and given regular media coverage.

The DPO will maintain and update the register of breaches.