\*\* FREE PREVIEW VERSION \*\*

[organization logo]

[organization name]

**DATA BREACH RESPONSE AND NOTIFICATION PROCEDURE**

|  |  |
| --- | --- |
| Code: |  |
| Version: |  |
| Date of version: |  |
| Created by: |  |
| Approved by: |  |
| Confidentiality level: |  |

**Change history**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Version** | **Created by** | **Description of change** |
| dd.mm.yyyy | 0.1 | EUGDPRAcademy | Basic document outline |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Table of contents**

[1. Scope, purpose and users 3](#_Toc499196655)

[2. Reference documents 3](#_Toc499196656)

[3. Definitions 3](#_Toc499196657)

[4. Data Breach Response Team 4](#_Toc499196658)

[5. Data Breach Response Team duties 5](#_Toc499196659)

[6. Data Breach Response process 5](#_Toc499196660)

[7. Personal data breach notification: Data processor to data controller 5](#_Toc499196661)

[8. Personal data breach notification: Data controller to supervisory authority 6](#_Toc499196662)

[9. Personal data breach notification: Data controller to data subject 6](#_Toc499196663)

[10. Accountability 7](#_Toc499196664)

[11. Managing records kept on the basis of this document 7](#_Toc499196665)

[12. Validity and document management 7](#_Toc499196666)

# 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.

The Procedure lays out the general principles and actions for successfully managing the response to a data breach as well asfulfilling 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 [Company Name] (“Company”) must be aware of, and follow this Procedure in the event of a personal data breach.

# 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 with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC)
* [relevant national law or regulation for GDPR implementation]
* [other local laws and regulations]
* Personal Data Protection Policy

# 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.

**“Processor”** is a natural or legal person, public authority, agency or any other body which processes personal data on behalf of a Data Controller.

**“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.

\*\* END OF FREE PREVIEW \*\*

To download full version of this document click here: <https://advisera.com/eugdpracademy/documentation/data-breach-response-and-notification-procedure/>