Data Breach Policy

Personal data breach notification procedure

Date of last policy revision: 25/9/2018

CONTENTS

1. PREMISES

The **Libera Università di Lingue e Comunicazione IULM**, pursuant to Regulation (EU) 2016/679 (hereinafter GDPR), is obliged to keep safe the personal data processed within the scope of its institutional activities and to act without undue delay in the event of a data breach (including notifications to the competent Data Protection Authority and notifications to the data subjects).
It is of paramount importance to prepare courses of action to be implemented in the event of actual, potential or suspected breaches of personal data, in order to avoid risks to the rights and freedoms of the data subjects, as well as economic damage to the University, and to be able to notify the Supervisory Authority and/or the data subjects within the timeframe and in the manner provided for by the European legislation.
The sanctions provided for by the GDPR for failure to notify a Data Breach to the Supervisory Authority or failure to notify the data subjects or both, in cases where the requirements of Articles 33 and 34 GDPR are met, may result in the imposition on the Libera Università di Lingue e Comunicazione IULM of an administrative fine of up to EUR 10 million or up to 2% of the total annual "turnover" of the previous year, also accompanied by a corrective measure pursuant to Article 58 c. 2.

2. PURPOSE

The purpose of this procedure is to draw up a flowsheet for the management of personal data breaches processed by the Libera Università di Lingue e Comunicazione IULM in its capacity as Data Controller (hereinafter referred to as **'Data Controller'**). These procedures are in addition to the procedures adopted by the Data Controller for the protection of personal data under current legislation.

3. WHAT IS A DATA BREACH?

A personal data breach is any breach of data security leading - accidentally or unlawfully - to the destruction, loss, alteration, unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed by the Data Controller.

Personal data breaches can occur for a wide range of reasons that may include:

- disclosure of confidential data to unauthorised persons;
- loss or theft of data or of devices in which data are stored;
- loss or theft of paper documents;
- corporate disloyalty (e.g. a data breach caused by an internal employee having authorisation to access the data, making a copy of it and distributing it in a public environment)
- unauthorised access (e.g. a data breach caused by unauthorised access to computer systems with subsequent disclosure of the acquired information);
- cases of hacking;
- databases altered or destroyed without authorisation from the related 'owner';
- viruses or other attacks on the computer system or corporate network;
- violation of physical security measures (e.g. forcing open doors or windows of security rooms or archives containing confidential information);
- loss of company laptops, devices or IT equipment;
- sending e-mails containing personal and/or sensitive data to the wrong recipient.

4. WHO ARE THESE PROCEDURES FOR?

These procedures are addressed to all entities that in any capacity process personal data for which the **Data Controller** is responsible (as better described in Section 5 of this procedure), such as:

- employees, as well as those who for any reason - and therefore regardless of the type of relationship - have access to personal data processed in the course of their employment on behalf of the Data Controller (hereinafter generically referred to as Internal Recipients)
- any person (natural person or legal entity) other than the internal Recipient who, by reason of the contractual relationship in place with the Data Controller, has access to the aforementioned data and acts in the capacity of Data Processor pursuant to Article 28 GDPR or as an autonomous Data Controller (hereinafter generically referred to as External Recipients);

  hereinafter generically referred to as 'Recipients'.

All Recipients must be duly informed of the existence of this procedure, by methods and means that ensure comprehension thereof.

Compliance with this procedure is compulsory for all those involved, and failure to comply with the rules of conduct laid down herein may result in disciplinary measures being taken against defaulting employees or in the termination of existing contracts with defaulting third parties, in accordance with the regulations in force.

5. WHAT TYPES OF DATA DO THESE PROCEDURES REFER TO?

These procedures refer to:

- personal data processed 'by' and 'on behalf of' the Data Controller, in any format (including paper documents) and by any means;
- personal data stored or processed by means of any other business system.

'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.*

6. NOTIFICATION OF DATA BREACHES

Personal data breaches are managed by the Data Controller or their delegate under the supervision of the DPO.

In the event of a concrete, suspected and/or actual personal data breach, it is of the utmost importance to ensure that it is addressed immediately and correctly in order to minimise the impact of the breach and prevent its recurrence.

In the event that one of the Recipients becomes aware of a concrete, potential or suspected personal data breach, they must immediately **inform their line manager of the incident**, who will then, with the support of the Recipients themselves, inform the Data Controller or their delegate by filling in the **Internal Data Breach Notification Form** (**Annex A) -** to be sent by email to databreach@iulm.it .

7. DATA BREACH MANAGEMENT

To manage a personal data breach, the following four steps must be followed:

Step 1: Identification and preliminary investigation

Step 2: Containment, recovery and risk assessment

Step 3: Notification to the Supervisory Authority

Step 4: Communication to the data subject

Step 5: Documenting the breach

Step 1: Identification and preliminary investigation

Annex A, duly completed, will enable the Data Controller or their delegate to conduct an initial assessment of the report of the incident that occurred, in order to establish whether a data breach has actually occurred and whether a more in-depth investigation of the incident is required, proceeding with the risk assessment (step 2) and with the involvement of the DPO.

In the event of a breach of data contained in an IT system, the Data Controller or their delegate **must also involve the Head of the IT Department, or their delegate in the event of their absence, in the entire procedure described in this document.**

This initial assessment will be carried out by examining the information in Annex A, namely:

- The date of discovery of the breach (promptness);
- The person who became aware of the breach;
- The description of the incident (nature of the breach and the data involved);
- The categories and approximate number of data subjects involved in the breach;
- The description of any actions already taken.

Step 2: Containment, Recovery and Risk Assessment

Once it has been established that a Data Breach has occurred, the Data Controller or their delegate together with the DPO must establish:

- whether there are actions that could limit the damage that the breach could cause (e.g. physical repair of equipment; use of back-up files to recover lost or damaged data; isolation/closure of a compromised sector of the network; change of access codes, etc.);
- once these actions have been identified, who should act to contain the breach;
- whether it is necessary to notify the Data Protection Authority of the breach (where the breach is likely to present a risk to the rights and freedoms of natural persons);
- whether it is necessary to notify the data subjects of the breach (where the breach presents a high risk for the rights and freedoms of natural persons).

In order to identify the need to notify the Data Protection Authority and the data subjects, the Data Controller and the DPO will assess the seriousness of the breach using the **Data Breach Risk Assessment**

Form (Annex B), which must be examined together with Annex A, also taking due account of the principles and indications set out in Article 33 GDPR.

If, in fact, the obligation to notify the Supervisory Authority arises once a simple risk threshold has been exceeded, Article 34 GDPR, on the other hand,requires that the obligation to notify the data subjects be triggered once a high risk has been exceeded.

Step 3: Notification to the competent Supervisory Authority

Once it has assessed the need to notify the data breach incurred on the basis of the procedure described in step 2, in accordance with the provisions of Regulation (EU) 2016/679, **the Libera Università di Lingue e Comunicazione IULM** shall do so, without undue delay and, where possible, within 72 hours from the moment it became aware of the breach.

Consequently, the Data Controller and the DPO will identify the competent Supervisory Authority on the basis of the privacy policies and/or of the data protection impact assessment already in place at the Libera Università di Lingue e Comunicazione IULM in relation to the data affected by the breach (in the absence of any documentation identifying the competent Supervisory Authority beforehand, the Data Protection Authority shall be that of the State where the main or sole establishment of the Data Controller is located, also for any cross-border processing operations that may be carried out).

Once the competent Supervisory Authority has been determined, the Data Controller and the DPO will decide on the correct forms to be used to make the notification and will then proceed accordingly.

Step 4: Communication to the data subject

Once the need to notify the data breach to those whose data is being processed has been assessed, on the basis of the procedure referred to in step 2, in accordance with the provisions of Regulation (EU) 2016/679, the **Libera Università di Lingue e Comunicazione IULM** shall do so, without undue delay.

As regards the content of this communication, the Data Controller or their delegate and the DPO must:

- provide the name and contact details of the Data Protection Officer (DPO);
- describe the likely consequences of the personal data breach
- describe the measures taken or proposed by the Data Controller to remedy the personal data breach and, where appropriate, to mitigate its possible adverse effects.

Regarding notification procedures, on a case-by-case basis, the Data Controller or their delegate and the DPO should always favour direct communication with the data subjects (such as e-mail, SMS or direct messages). The message should be communicated in a clear and transparent manner, which means avoiding sending the information in the context of general updates or newsletters, which could be easily misunderstood by the recipients. In cases where direct notification requires an effort that is deemed disproportionate, then public communication may be used, which must be equally effective in contacting the interested party directly.

Step 5: Documenting the breach

Regardless of the assessment as to the need to proceed with the notification and/or communication of the Data Breach, whenever an incident communicated by the Recipients through Annex A occurs, the Libera Università di Lingue e Comunicazione IULM shall document it.

This documentation shall be entrusted to the Data Controller or their delegate with the assistance of the IT Department Manager (if the breach concerns data contained in IT systems), who shall do so by keeping the **Data Breach Register (Annex C)**, in accordance with the information contained therein: (i) number of breaches; (ii) date of breach; (iii) nature of breach; (iv) category of data subjects; (v) category of personal data involved; (vi) approximate number of personal data records; (vii) consequences of the breach; (viii) countermeasures adopted; (ix) whether notification was made to the Data Protection Authority; (x) whether communication was made to the data subjects.

The Data Breach Register must be continuously updated and made available to the Supervisory Authority, should the Authority request access to it.

ANNEX A - DATA BREACH NOTIFICATION FORM

If you discover a Data Breach, please inform your line manager immediately, who, in turn, should complete the form below and send it by e-mail to the following e-mail address: databreach@iulm.it.

Communication of Data Breach	**Notes**
Date breach was identified:	
Date of incident:	
Place of breach (specify whether it occurred as a result of lost devices or portable media):	
Name of the person who reported the breach:	
Contact details of the person who reported the breach (e-mail address, telephone number): *In the case of an external recipient, please indicate the company name:*	
Designation of the database(s) subject to the data breach and brief description of the breach of personal data contained therein:	
Categories and approximate number of interested parties involved in the breach:	
Brief description of any actions taken upon discovery of the breach:	
Head of department:	
date:	

ANNEX B - DATA BREACH RISK ASSESSMENT FORM

Risk Assessment Rating	To be compiled by the DPO together with the IT Department and the Head of the office involved in the breach
Devices subject to Data Breach (computer, mobile device network, file or part of a file, back-up tool, paper document, other).	
Types of exposure to risk (type of breach): reading (presumably the data have not been copied), copying (the data are still present on the owner's systems but have been copied), alteration (the data are present on the systems but have been altered), deletion (the data are no longer present and the perpetrator does not have them), theft (the data are no longer on the owner's systems and the perpetrator has them), other.	
Brief description of the processing or data storage systems involved, including their location.	
If a laptop is lost/stolen: when was the last time the laptop was synchronized with the central IT system?	
How many people were affected by the breach of personal data processed within the breached database?	
Could the breach have harmful consequences in one of the following areas of the University? Teaching Support, Student Services, Administration, Teaching, Research, Reputation	
What is the nature of the data involved? Please fill in the sections below:	
o Sensitive data (as specified by Regulation (EU) 2016/679 relating to a living, identifiable person): a) racial or ethnic origin b) political opinion, religious or philosophical beliefs; c) trade union membership; d) genetic data; e) biometric data; f) judicial data; g) relating to a person's health or sexual orientation.	

o Information that can be used to commit identity theft (e.g. access and identification data, social security number and copies of identity card, passport or credit cards);	
o personal information related to vulnerable persons (e.g. the elderly, the disabled, minors);	
o Individual profiles including information on job performance, salary or family status, disciplinary sanctions, which could cause significant harm to individuals	
Other:	
Could the breach result in damage to reputation, loss of confidentiality of data protected by professional secrecy, unauthorized decryption of pseudonymization, or any other significant financial or social data?	
Are data subjects at risk of being deprived of exercising control over personal data concerning them?	
What technical and organizational measures are taken regarding the breached data? (e.g. pseudonymisation and encryption of personal data)	
Has the Data Controller adhered to an approved code of conduct pursuant to Regulation (EU) Art. 40 or a certification mechanism pursuant to Regulation (EU) Art. 42?	
Has the Data Controller taken measures to prevent the occurrence of high risk for the rights and freedoms of data subjects after the breach?	
Classification of the breach (1, 2 or 3) and reasons:	
Notification of data breach to the Data Protection Authority	**YES/NO If yes, notified on: [date]** **Details:**
Communication of data breach to data subjects	**YES/NO If yes, notified on: [date]** **Details:**
Communication of data breach to other parties (e.g. managers)	**YES/NO If yes, notified on: [date]** **Details:**