PERSONAL DATA BREACH PROCEDURE

Introduction

Loyaltek SA is obliged under the GDPR to keep personal data safe and secure and to respond promptly and appropriately to data security breaches. It is vital to take prompt action in the event of any actual, potential or suspected breaches of data security or confidentiality to avoid the risk of harm to individuals, damage to operational business and severe financial, legal and reputational costs.

The purpose of this procedure is to provide a framework for reporting and managing data security
breaches affecting personal or sensitive personal data held by Loyaltek SA. This procedure is a supplement to our Data Protection Policy which affirms our commitment to protect the privacy rights of individuals in accordance with GDPR.

1. WHAT IS A PERSONAL DATA SECURITY BREACH?

A personal data security breach is any event that has the potential to affect the confidentiality, integrity or availability of personal data held by the Institute in any format. Personal data security breaches can happen for a number of reasons, including:

- the disclosure of confidential data to unauthorised individuals;
- loss or theft of data or equipment on which data is stored;
- loss or theft of paper records;
- inappropriate access controls allowing unauthorised use of information;
- suspected breach of Loyaltek's IT security;
- attempts to gain unauthorised access to computer systems, e.g. hacking;
- records altered or deleted without authorisation by the data "owner";
- viruses or other security attacks on IT equipment systems or networks;
- breaches of physical security e.g. forcing of doors or windows into secure room or filing cabinet containing confidential information;
- confidential information left unlocked in accessible areas;
- leaving IT equipment unattended when logged-in to a user account without locking the screen to stop others accessing information;
- emails containing personal or sensitive information sent in error to the wrong recipient.

2. WHAT TYPES OF DATA DO THESE PROCEDURES APPLY TO?

This procedure applies to:

- all personal data created or received by Loyaltek SA in any format (including paper records), whether used in the workplace, stored on portable devices and media, transported from the workplace physically or electronically or accessed remotely;

- personal data held on all Loyaltek IT systems.

3. PROCEDURE FOR REPORTING PERSONAL DATA SECURITY BREACHES

In the event of a breach of personal data security occurring, it is vital to ensure that it is dealt with immediately and appropriately to minimise the impact of the breach and prevent a recurrence.

If an employee of Loyaltek SA becomes aware of an actual, potential or suspected breach of personal
data security, he/she must report the incident to their Legal, IT and Support Department immediately.

The Legal, IT or Support Department Manager must then:
- report the incident immediately;
- complete the attached Data Security Breach Report Form (See Appendix 1)

This will enable all the relevant details of the incident to be recorded consistently and communicated on a need-to-know basis to relevant staff so that prompt and appropriate action can be taken to resolve the incident.

4. PROCEDURE FOR MANAGING DATA SECURITY BREACHES

In line with best practice, the following five steps should be followed in responding to a data security
breach:
- Step 1: Identification and initial assessment
- Step 2: Risk Assessment
- Step 3: Notification
- Step 4: Evaluation and Response

Step 1: Identification and initial assessment of the incident

If an employee of Loyaltek SA considers that a data security breach has occurred, this must be reported immediately to the Legal, IT or Support Department. The Legal, IT or Support Department Manager should complete part 1 of the Data Security Breach Report Form (Appendix 1) establishing:
- if a personal data security breach has taken place; if so:
- what personal data is involved in the breach;
- the cause of the breach;
- the extent of the breach (how many individuals are affected);
- the harms to affected individuals that could potentially be caused by the breach;
- how the breach can be contained.

Following this initial assessment of the incident, the Legal, IT or Support Department Manager will, investigate the incident. The Legal, IT or Support Department Manager will determine the severity of the incident using the checklist in Appendix 2 and by completing part 2 of the Data Security Breach Report Form (Appendix 1).

The severity of the incident will be categorised as level 1, 2 or 3:

- Level 1 classed as a Local Incident
- Level 2 classed as a Minor Emergency
- Level 3 classed as a Major Emergency

Step 2: Risk Assessment

The Legal, IT or Support Department Manager will review the incident report to:

- Assess the risks and consequences of the breach;
- Determine, where appropriate, what further remedial action should be taken on the basis of the incident report to mitigate the impact of the breach and prevent repetition.

Step 3: Notification

On the basis of the evaluation of risks and consequences, the Legal, IT or Support Department Manager, and others involved in the incident as appropriate, will determine whether it is necessary to notify the breach to the Data Protection Authority and/or the data subject.

In accordance with GDPR all incidents in which personal data has been put at risk should be reported to the Data Protection Authority (“DPA”) as soon as the Company becomes aware of the incident.
Personal data breach notifications to the DPA must be made by the appointed person (Legal, IT or Support Department Manager) using the form set out in appendix 1. The appointed person must keep a record of all notifications and communications with the DPA.

In cases where the decision made by the Legal, IT or Support Department Manager is not to report a breach, a brief summary of the incident with an explanation of the basis for not informing the Data Protection Authority will be retained by the Legal Officer.

Step 4: Evaluation and Response

For each serious incident, the Legal, IT or Support Department Manager will conduct a review to
consider and report to the Managing Director on the following:

- What action needs to be taken to reduce the risk of future breaches and minimise their impact?
- Whether policies procedures or reporting lines need to be improved to increase the effectiveness of the response to the breach?
- Are there weak points in security controls that need to be strengthened?
- Is additional investment required to reduce exposure and if so what are the resource implications?
-

5. Data Protection Authority

Rue de la Presse 35, 1000 Brussels, Belgium
Phone : +32 (0)2 274 48 00
Mail : contact(at)apd-gba.be

APPENDIX 1 – PERSONAL DATA SECURITY BREACH REPORT FORM

Section 1: Notification of Data Security Breach	To be completed by Legal, IT or Support Department Manager
Date incident was discovered:	
Date(s) of incident:	
Place of incident:	
Name of person reporting incident:	
Contact details of person reporting incident	
Brief description of incident or details of the information lost:	
Number of Data Subjects affected, if known:	
Has any personal data been placed at risk? If, so please provide details	
Brief description of any action taken at the time of discovery:	
For Company use	

Received by:	
On (date):	
Forwarded for action to:	
On (date):	

Section 2: Assessment of Severity	To be completed by Legal, IT or Support Department Manager
Details of the IT systems, equipment, devices, records involved in the security breach:	
Details of information loss:	
What is the nature of the information lost?	
How much data has been lost?	
Is the information unique? Will its loss have adverse operational, research, financial legal, liability or reputational consequences for the Institute or third parties?	
How many data subjects are affected?	
Is the data bound by any contractual security arrangements ?	
What is the nature of the sensitivity of the data?	
HIGH RISK personal data - Sensitive personal data : a) racial or ethnic origin; b) political opinions or religious or	

philosophical beliefs; c) membership of a trade union; d) physical or mental health or condition or sexual life; e) commission or alleged commission of any offence, or f) proceedings for an offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings.	
Information that could be used to commit identity fraud such as personal bank account and other financial information and national identifiers and copies of passports and visas;	
Personal information relating to vulnerable adults and children;	
Detailed profiles of individuals including information about work performance, salaries or personal life that would cause significant damage or distress to that person if disclosed;	
Spreadsheets of marks or grades obtained by students, information about individual cases of student discipline or sensitive negotiations which could adversely affect individuals.	

Security information that would compromise the safety of individuals if disclosed	
Category of incident (1, 2 or 3):	

Section 3: Action taken	To be completed by Legal, IT or Support Department Manager
Incident number	
Report received by:	
On (date):	
Action taken by responsible officer/s :	
Notification to Data Protection Authority	YES/NO If YES, notified on:
Notification to data subjects	YES/NO If YES, notified on:

APPENDIX 2 – CHECKLIST FOR ASSESSING SEVERITY OF THE INCIDENT

Level 1 - Local Incident

Local incident = limited disruption to services (department, building or Institute); no serious threat to life, property or the environment; no threat to Loyaltek's image/reputation.

Can the consequences of the security breach, loss or unavailability of the asset be managed locally within normal operating procedures? If so, manage the incident according to the Data Security Breach Management Procedure (this procedure).

Level 2 - Minor Emergency

Minor Emergency = Disruption to the functioning capacity of a key service. Situation or incident (actual or potential) which poses a threat to life, property or environment.

- Do containment and recovery require assistance from other members of staff ?
- Does the breach require a notification to the Managing Director ?

Level 3 - Major Emergency

The incident level is defined by:

- Does the incident need to be reported immediately to the DPA ?
- Is it business-critical? Do you rely on access to this particular information asset or you can turn to reliable electronic copies or alternative manual processes ?
- How urgently access would need to be restored to an information asset to resume business or, if a workaround will keep business moving in the short term, to return to the required standard of service ?
- Does the loss or breach of data security involve high risk personal data ?

  - Sensitive personal data relating to a living, identifiable individual's :

  a) racial or ethnic origin;
  b) political opinions or religious or philosophical beliefs;
  c) membership of a trade union;
  d) physical or mental health or condition or sexual life;
  e) commission or alleged commission of any offence, or
  f) proceedings for an offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings.

  - Information that could be used to commit identity fraud such as personal bank account and other financial information and national identifiers (e.g.: copies of passports and visas);
  - Personal information relating to vulnerable adults and children;
  - Detailed profiles of individuals; including information about work performance, salaries or personal life that would cause significant damage or distress to that person if disclosed;
  - Security information that would compromise the safety of individuals if disclosed.