Swiss International Institute Lausanne

DATA BREACH NOTIFICATION – PROCEDURAL GUIDELINES

Swiss International Institute Lausanne - SIIL

Approved by:	Academic Council
Date of Approval:	01.09.2022
Date of Next Review:	01.09.2025
Owner:	IT Office
Contact:	p.tkachev@siil.ch

DATA BREACH NOTIFICATION – PROCEDURAL GUIDELINES

Swiss International Institute Lausanne - SIIL

Table of contents

I INTRODUCTION

Swiss International Institute Lausanne – SIIL (SIIL – HEI) is required under data protection legislation to keep personal data safe and secure and to respond promptly and appropriately in the event of a breach of security relating to personal data (hereinafter 'data breach').

The purpose of these Procedural Guidelines is to provide a framework for reporting and managing breaches involving personal data controlled and processed by the HEI. The Guidelines supplement the SIIL *Data Protection Policy* which affirms the SIIL's commitment to protect the privacy rights of individuals in accordance with Swiss data protection legislation, as well as the EU General Data Protection Regulation ('GDPR') (if applicable).

Where a data breach is likely to result in a risk to the rights and freedoms of data subjects, the HEI is required under GDPR (when applicable) to report the breach to the Data Protection Officer **within 72 hours of discovery, even if the risk is not considered as substantial**.

Where appropriate, actions to inform data subjects affected by the breach and reduce risks to their privacy arising from the breach must also be implemented without delay, pursuant to Article 34 GDPR.

These timeframes include weekend and public holidays and failure to comply will result in regulatory sanction and reputational damage for SIIL.

As such, it is extremely important that you take immediate action upon learning of a breach or suspected incident involving the loss or disclosure of data and contact the Data Protection Officer at dpo@siil.ch and Head of Department / Unit without delay. All emails should be marked 'Urgent'.

If unsure whether an incident is a data breach or not, please, refer to the guidance set out within this document and consult with the DPO.

II SCOPE

These Guidelines apply to individuals who process personal data on behalf of SIIL, including:

- Any individual who is employed by SIIL or is engaged by SIIL who has access to SIIL-controlled or processed personal data in the course of their employment or engagement for administrative, research and/or any other purpose;

- Any student of SIIL who has access to SIIL-controlled or processed personal data in the course of their studies for administrative, research and/or any other purpose; or

- Individuals who are not directly employed by SIIL, but who are employed by contractors (or subcontractors) and who have access to SIIL-controlled or processed personal data in the course of their duties for the Institute.

These Guidelines apply to:

- All personal data processed by SIIL in any format (including electronic and paper records), whether used in the workplace including working from home, stored on portable devices and media, transported from the workplace physically or electronically, or accessed remotely;
- Personal data held on all SIIL IT systems and software solutions, including Cloud- based platforms, managed centrally by IT Services or locally by individual Schools/ Departments/ Offices/ Institutes or Centres;
- Any other IT systems, including email and Cloud-based platforms on which SIIL-controlled or processed personal data is processed.

III DEFINITIONS AND TERMINOLOGY: WHAT IS A DATA BREACH?

Under GDPR and Swiss legislation having implemented this directive, a **data breach** is defined as 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. This definition extends to breaches which result from malicious conduct, lack of appropriate security controls, system or human failure, or error.

Data breaches may occur in a variety of contexts. For example:

- Disclosing confidential data to unauthorised individuals. For example, accidentally sending an email containing confidential or sensitive data to the wrong recipient or recipients as a result of human error.
- Loss or theft of data, including equipment on which data is stored (e.g. laptop, smartphone, tablet USB key etc.) or paper records.
- Inappropriate access controls allowing unauthorised use of information (e.g. uploading personal data to an unsecured web domain, using unsecure passwords).
- Equipment failure.
- Confidential information left unlocked in accessible areas (e.g. leaving IT equipment unattended when logged into a user account).
- Collection of personal data by unauthorised individuals.
- Hacking, viruses or other security attacks on IT equipment, systems or networks.
- Breaches of physical security (e.g. forcing of doors/ windows/ filing cabinets).

Whether an incident giving rise to the suspected data breach involves personal data must be determined on a case-by-case basis. If an incident does not involve personal data, it is not a data breach per the GDPR definition. Furthermore, not all data incidents involving personal data will be data breaches.

For example:

- The personal data is securely encrypted or anonymised so as to make the personal data unintelligible; and/or
- There is a full, up-to-date back-up of the personal data (in cases of accidental destruction).

If there is any doubt as to whether a data breach has occurred, the DPO (Data Protection Officer) should be consulted immediately.

Personal data is defined under GDPR as:

'*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*'.

Special categories of personal data are defined under GDPR as:
'Personal data revealing racial origin, ethnic origin, political opinions, religious beliefs, philosophical beliefs, trade-union membership, genetic and biometric data which is processed for the purpose of uniquely identifying a natural person, data concerning health, data concerning a natural person's sex life and data concerning a natural person's sexual orientation'.

Processing is defined under GDPR as:
*'Any operation or a set of operations which is performed on personal data or on sets of personal data, whether or not 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'.*

IV PROCEDURE TO REPORTING A DATA BREACH

According to the Swiss legislation and unlike the Article 33 GDPR (when applicable) with the strict frame of 72 hours, SIIL must report a data breach, if deemed reportable, to the Data Protection Officer **as soon as possible**.

This timeframe includes weekends and bank holidays.

Under Article 34 GDPR when applicable SIIL must inform affected individuals **without undue delay** if the data breach is likely to result in a high risk to their privacy.

As such, any data breach must be dealt with immediately and appropriately. If a member of SIIL becomes aware of an actual, potential or suspected data breach, they must report the incident to the Data Protection Officer at dpo@siil.ch and to their Head of Department/ Head of Unit immediately. All emails should be marked 'Urgent'.

The DPO is responsible for keeping a written record of all potential or suspected data breaches that are notified to him/ her.

V PROCEDURE TO MANAGING A DATA BREACH

Upon receiving notification of a data breach, the DPO shall, in conjunction with appropriate members of staff, take the following five steps (in line with best practice) when responding to the incident:

- **Step 1: Identification and initial assessment of the incident**
- **Step 2: Containment & recovery**
- **Step 3: Risk assessment**
- **Step 4: Notification**
- **Step 5: Evaluation & response**

1. Step 1: Identification & Initial Assessment of the Incident

If any member of SIIL considers that a data breach has, or might have, occurred, they must report the incident immediately to the DPO.

The DPO will conduct an initial assessment of the incident. This assessment will take into account:

- Whether a data breach has taken place.
- The nature and type of the personal data involved in the breach, including whether sensitive or confidential personal data has been compromised.
- The cause of the breach.
- The extent of the breach (i.e. the number of individuals affected).
- The potential harms to which affected individuals may be exposed.
- Any steps that may be taken to contain the breach.

Following this initial assessment of the incident, the DPO may, according to the severity of the incident, consult with the Rectorate and decide if it is necessary to appoint a group of relevant SIIL stakeholders (e.g. IT Services, Financial Services Division, Human Resources, Academic Registry) to assist with the investigation and containment process.

2. Step 2: Containment & Recovery

In the event of a data breach, immediate and appropriate steps must be taken to limit the extent of the breach.
The DPO, in consultation with relevant staff, will:

- Establish who within SIIL needs to be made aware of the breach (e.g. IT Services, Operations Office) and inform them of their expected role in containing the breach (e.g. isolating a compromised section of the network, notifying affected individuals).
- Establish whether there is anything that can be done to recover any losses and limit the damage caused by the breach.
- Where appropriate, inform the competent authorities (e.g. in cases involving criminal activity).

3. Step 3: Risk Assessment

The DPO, in conjunction with relevant staff, will use the information provided to fulfil the requirement to assess the potential adverse consequences for individuals, including how likely such adverse consequences are to materialise and how serious or substantial they are likely to be.

This assessment should, in particular, consider the likelihood of risks taking place and the severity of such risks is to be categorised as no risk/ risk/ high risk in accordance with the detailed criteria below:

- **Nature of the breach**: destruction, damage or any other form of unauthorised, accidental or unlawful access to, collection, use, recording, storing or distributing of personal data. What type of a data breach has or may have occurred? Does the breach consist of a breach of confidentiality relating to personal data? Is there a temporary or permanent lack of availability or access to personal data and if temporary, how long will it be before it is restored?
- **Nature of personal data:** Is the relevant personal data sensitive in nature? The more sensitive the personal data the higher the risk of the data breach. The utility of the relevant information may also indicate a higher risk to the affected individuals.
- **Scale and volume of personal data affected:** The higher the volume of the personal data records and the number of individuals potentially affected will usually create a higher risk.
- **Ease of identification:** The ease of identifying the relevant individuals based on the personal data will likely increase the risk of identity theft, fraud and reputational damage in particular.
- **Security measures:** Are the risks arising from the breach limited as a result of inherent security measures, such as encryption, where the confidentiality of the key is still intact and the data is unintelligible to a third party?
- **Containment measures:** Have any containment measures been implemented which means that the data breach is unlikely to present a risk to the individuals affected?

- **Other factors:** Other relevant factors in assessing the risk to individuals are whether those individuals affected by the data breach have any special characteristics (for example, children or vulnerable adults).
- **Severity of risk:** Based on the above criteria and any other relevant factors, the DPO should assess the severity of the risk in terms of the potential consequences to the individuals affected by the data breach.
- **Likelihood of the risk(s) materialising:** Once the data breach has occurred, the DPO must objectively assess the likelihood of the potential risks actually materialising and this should form part of the risk assessment.
- **An assessment of the risks for SIIL**, including strategic and operational, legal, financial and reputational risks may also be prepared.

4. Step 4: Notification

Under the Swiss legislation SIIL must report a data breach as soon as possible if deemed reportable, to the Data Protection Officer of becoming aware of the breach. **This timeframe includes weekends and bank holidays.**

If a decision is made to not report a breach, a summary record of the incident with an explanation of the basis for not informing retained by the DPO.

Affected individuals: Under Article 34 GDPR when applicable SIIL must inform affected individuals without undue delay if the data breach is likely to result in a high risk to their privacy.

Where the DPO assesses that there is a high risk to rights and freedoms of individuals as a result of the data breach, then the existence of the data breach should be communicated to the affected individuals without undue delay.

Any such communication should inform the affected individuals on relevant measures that they can take to reduce the risks to them and any negative consequences arising from the data breach. The DPO should determine the most appropriate and effective means of communicating the data breach to the affected individuals and engaging the assistance of communications advisors if appropriate.

Notification should have a clear purpose, to enable individuals who may have been affected to take appropriate steps to protect themselves (e.g. by cancelling a credit card or changing a password), to allow regulatory bodies to perform their functions, provide advice and deal with complaints. In each case, the notification should include as a minimum:

- a description of the nature of the breach;
- a description of the likely consequences of the breach;
- how and when the breach occurred;
- what data was involved;

- a description of the measures taken or proposed to be taken by the University to address the breach; and
- the name and contact details of the DPO and other contact points.

Other parties: SIIL should consider, and seek advice as appropriate, as to whether there are any other relevant notification requirements required (such as to the competent authorities, insurers, external legal advisers etc.).

5. Step 5: Evaluation & Response

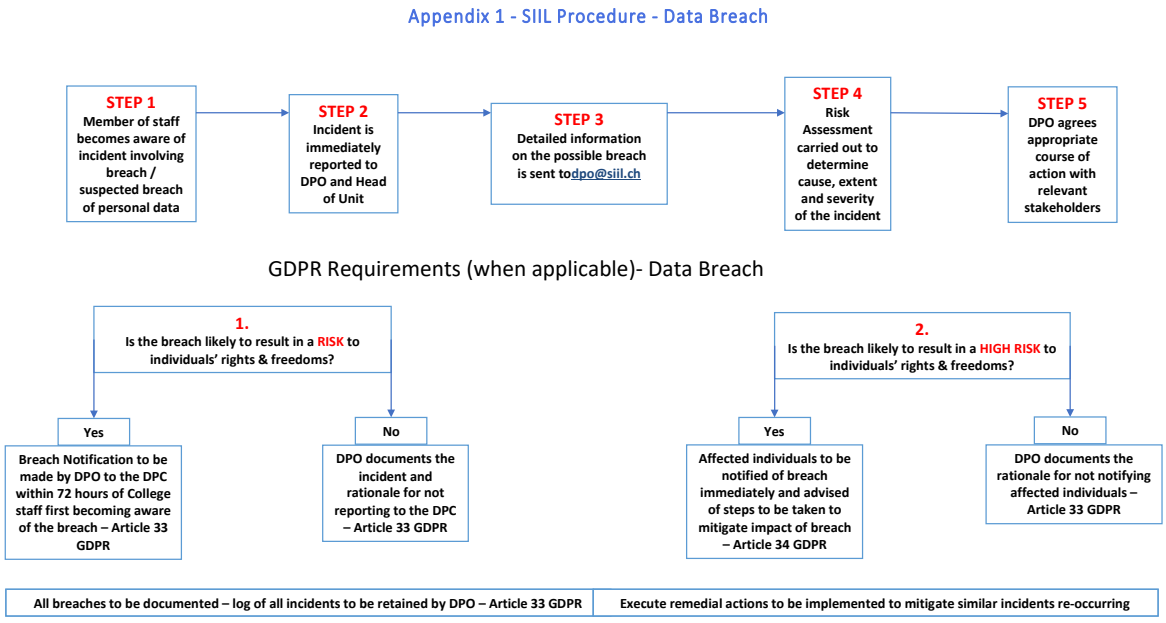
Certain data breaches will require further detailed investigation after the initial investigation period, which may involve external IT, legal and other support, as appropriate to ascertain the full extent of the data breach, its causes, likely consequences and in order to effectively contain the breach. The effect of the data breach must be monitored and the risks re-evaluated throughout this period. It may be necessary to agree a phased notification programme with the Data Protection Officer in these instances.

In the aftermath of a data breach, a post-incident review of the incident should take place to ensure that the steps taken during the incident were appropriate and effective, and to identify any areas that may be improved in future, such as updating policies and procedures or addressing systematic issues if they arise, in order to reduce the recurrence of similar data breaches and to ensure that appropriate technical and organisational security measures are put in place.

VI GUIDANCE

For further information and advice about what to do in the event of a suspected data breach please contact: Data Protection Officer, SIIL, Switzerland. Email: dpo@siil.ch.

VII APPENDIX 1. SIIL PROCEDURE – A DATA BREACH



Approved by:	Academic Council
Date of Approval:	01.09.2022
Date of Next Review:	01.09.2025
Owner:	IT Office
Contact:	p.tkachev@siil.ch