Data Breach Reporting Policy

Overview

This policy is to provide CIEE's procedures regarding an actual or suspected data breach involving personal information. CIEE has obligations under the GDPR and other international and domestic data privacy laws to ensure the correct procedures, controls and measures are in place and that all staff are aware of what the protocols and reporting requirements are regarding personal data breaches.

Purpose

This policy applies in the event of an actual or suspected security incident or data breach. Reporting incidents in full and with immediate effect is essential to the compliant functions of CIEE. This policy is for the protection of CIEE, its staff, customers, clients and third parties and is of the utmost importance for legal regulatory compliance.

Policy Statement

The purpose of this policy is to provide a process to report any security incident or data breach involving unapproved access to personal data to ensure that the incident or breach is appropriately mitigated, documented, and managed. This policy applies to all staff within CIEE *(full and part time staff, temporary staff, any third-party representatives or sub-contractors, agency workers, volunteers, interns (paid and unpaid) and agents engaged with CIEE in the US or overseas).* Adherence to this policy is mandatory and non-compliance could lead to disciplinary action.

In the event that a suspected security incident or data breach has occurred, reporting staff is required to:

1. Notify your direct line manager and together complete Part 1 of the Data Breach Reporting Form that can be found on the Policies & Required Postings page of the HR website. Upon completion of Part 1 please email a copy to dpo@ciee.org
2. Encrypt the email by including [**encrypt**] in the subject line of the email.
3. A ticket in Jira will be created on your behalf.
4. Upon receipt the Data Protection Officer will start an investigation with other parties (IT, Legal, Outside Counsel).

Incidents that require reporting:

- LOSS OR THEFT OF EQUIPMENT (LAPTOPS, MOBILE DEVICES, TABLETS)
- LOSS OR THEFT OF PRINTED MATERIALS THAT CONTAIN PERSONAL DATA
- UNAUTHORIZED ACCESS TO EQUIPMENT, SOFTWARE/APPLICATIONS OR PRINTED MATERIALS THAT CONTAIN PERSONAL DATA
- SENDING/SHARING PERSONAL DATA WITH AN INCORRECT PARTICIPANT