University College Dublin
An Coláiste Ollscoile, Baile Átha Cliath

Privacy Notice - UCD's Security Incident & Event Management (SIEM) Deployment

Introduction

UCD is committed to protecting the privacy and security of personal data in accordance with the General Data Protection Regulation (GDPR). This privacy statement outlines how we handle personal data in the context of our SIEM system and associated processes, which is used to enhance the security of UCD's digital environment. The SIEM is a sectoral solution, data is collected and analyzed via network monitoring and log files from UCD's IT environment. Data is analysed for incidents by an external company and

Purpose and Legal Basis

The purpose of processing personal data through UCD's SIEM system is to ensure the security and integrity of our digital environment. This includes monitoring for potential security threats and incidents, and maintaining compliance with relevant regulations. The legal basis for this processing is our legitimate interest in securing our digital environment and protecting the data of our students, staff, and visitors, as per Article 6(1)(f) GDPR .

Types of Data Collected

We collect and process personal data from various sources, including:

- **Login Data**: Information related to user logins and access to UCD's applications
- **Network Activity**: Data on network and device traffic and interactions with our IT infrastructure.
- **Log Files**: Records of system events and activities.
- **Devices**: Data related to the security posture of client devices (such as laptops, desktops, ..) accessing UCD's network and applications

Recipients of Personal Data

Personal data may be shared with the following parties:

- **SIEM Service Providers**: Companies contracted to manage and maintain our SIEM system, with whom we have processor agreements.
- **IT Security Personnel**: Internal and external teams responsible for monitoring and responding to UCD's IT security incidents.
- **Regulatory Bodies**: As required by law or to comply with legal obligations.

Data Protection Measures

Access to data is restricted to authorized personnel, and all data handling activities are logged and monitored. The data itself is only accessed when an incident occurs requiring examination of the logged data. Only the data related to the incident is searched.We implement data protection by design and default.

Data Retention

Personal data collected through our SIEM system is retained for a period of 183 days unless otherwise required by law or for ongoing investigations.

International Data Transfers

All data processing and storage occur within the European Economic Area (EEA), ensuring compliance with GDPR requirements for international data transfers.

Date	Version	Approved By
May 2025	1	IT Security Manager