PROCEDURE FOR HANDLING DATA BREACHES

3 February 2016

Anyone who discovers a potential data breach will have to carry out an investigation quickly and may also have to notify the authorities and affected individuals.

Employees of the University of Twente must report the data breach as soon as possible, via cert@utwente.nl or ICT Service Desk (LISA) servicedesk-ict@utwente.nl tel. 5577.

Employees of the ICT Service Desk are on the alert for potential data breaches, such as: loss of a USB flash drive, theft of a laptop or an intrusion by a hacker and shall report security breaches via email to cert@utwente.nl. In urgent cases, call the CERT-UT employee on duty.

CERT-UT registers every report in the AIRT (Application for Computer Security Incident Response) system. This is a workflow application used by CERT-UT to keep a record of security breaches and incidents. CERT-UT then contacts the notifier for additional information about the report.

The CERT-UT employee on duty carries out a first analysis. In case of personal data, the incident is reported to the Security Manager (LISA), Data Protection Officer (FG) and Privacy Contact Person (PCP) of the unit. The security incident is assigned a type, making it identifiable as a privacy incident. CERT-UT takes care of handling the security incident, for which evidence or information for processing the data breach is stored in a safe environment. The Security Manager takes care of handling the privacy incident.

Together with the FG and the PCP, the Security Manager (LISA) assesses as to whether the incident must be reported to the Authority for Personal Data, and possibly also to the party concerned. If it is concluded that the incident must be reported to the Authority for Personal Data (AP), then the Security Manager shall first contact the secretary of the university prior to filing the report.

Reports to the AP are submitted by the Security Manager (LISA), at which time the status in AIRT is updated. If notifying the parties concerned is necessary, this shall be done by the PCP.

WHEN TO REPORT?

For a detailed description of the assessment as to whether a report should be filed, see the Policy of the Authority for Personal Data.