UT procedure for handling data breaches - version 2.0, 19 October 2020

When an organization like the University of Twente discovers a possible data breach, it will have to conduct an investigation, take measures and possibly also notify the Dutch Data Protection Authority (Dutch DPA) and data subjects.

Discovery and reporting of security incidents and data breaches

UT employees and students must therefore report a security incident or a possible data breach as soon as possible to CERT-UT at cert@utwente.nl, tel. 1313. This email address is also monitored outside office hours.

Employees of the ICT Service Desk are alert to potential data breaches, such as the loss of a USB flash drive, theft of a laptop or intrusion by a hacker. If necessary, they report security incidents by e-mail to cert@utwente.nl. In urgent matters they call the CERT-UT employee on duty.

CERT-UT registers every report and, if necessary, contacts the employee who summited a report where additional information is required.

Analysing and assessing data breaches

CERT-UT conducts an analysis and if it concerns personal data, it notifies the Security Manager (LISA). The Security Manager assesses the incident and if he thinks it is a data breach, he contacts the Data Protection Officer (DPO, in Dutch FG: Functionaris Gegevensbescherming)[1]. The DPO will contact the Privacy Contact Person (PCP) of the relevant unit. The DPO is responsible for the handling of the data breach, for which evidence or information regarding the breach is stored in a safe environment.

Together with the Security Manager, the PCP of the relevant unit and the stakeholder of the incident, the DPO includes the data breach in the register of data breaches. CERT-UT handles the security incident underlying the data breach. Normal escalation procedures will be followed regarding the security incident.

If the DPO considers the data breach likely reportable to the Dutch DPA, the DPO will contact the member of the Executive Board responsible for business management. Reports to the Dutch DPA are submitted by the DPO. The PCP notifies the concerned parties. The report is archived in the register of data breaches by the DPO.

When to report to the Dutch DPA?

A data breach must be reported to the Dutch DPA, if the data breach results in a risk to the rights and freedoms of natural persons. When assessing risk, consideration should be given to at least:[2]

- the type of breach;

[1] One can only speak of a data breach when an actual security breach has occurred. A security breach may, for example, be the loss of a USB-key, the theft of a laptop or intrusion by a hacker. However, not every security breach comprises a data breach. A security breach is considered to be a data breach if it involves the loss of personal data, or if unlawful processing of personal data cannot reasonably be excluded. If there is only a weak spot in security, we speak of a vulnerability or a security incident and not of a data breach.

[2] For more information, see chapter IV of the Guidelines on Personal data breach notification.

- the nature, sensitivity and volume of personal data (for example special categories of personal data[3]);
- the ease of identification of individuals;
- the severity of consequences for individuals;
- special characteristics of the individual;
- special characteristics of the data controller;
- the number of data subjects.

In case the data breach needs to be reported to the Dutch DPA, this must be done without undue delay and if possible no later than 72 hours after having become aware of the data breach. For this purpose, a web form is available on the Dutch Data Protection Authority website. Reports can later be supplemented or withdrawn via this web form.

Notification to the data subject

If a data breach needs to be reported to the Dutch DPA, it does not necessarily require that the data subject of the breach be notified. If the data breach is likely to result in a high risk to the rights and freedoms of natural persons, the data subjects must be notified, unless an exception is provided in the GDPR. A high risk might involve physical, material or immaterial damage.

The flowchart attached as Annex 1 shows the notification requirements.

Other organisations

If other organisations are involved, for example when the UT is processing data on behalf of another party, this other organization will be notified of the data breach as soon as possible.

Report

Reporting of data breaches is part of the quarterly privacy report prepared by the DPO.

[3] Special categories of personal data are personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation (article 9 GDPR).

Annex 1 – Notification requirements