UT procedure for handling data breaches
Version 1.2, 26 March 2018

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 affected individuals.

UT employees must therefore report a security incident or a possible data breach as soon as possible to CERT-UT at cert@utwente.nl, tel 1313. CERT UT is also active outside office hours so they can act immediate upon a report.

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.

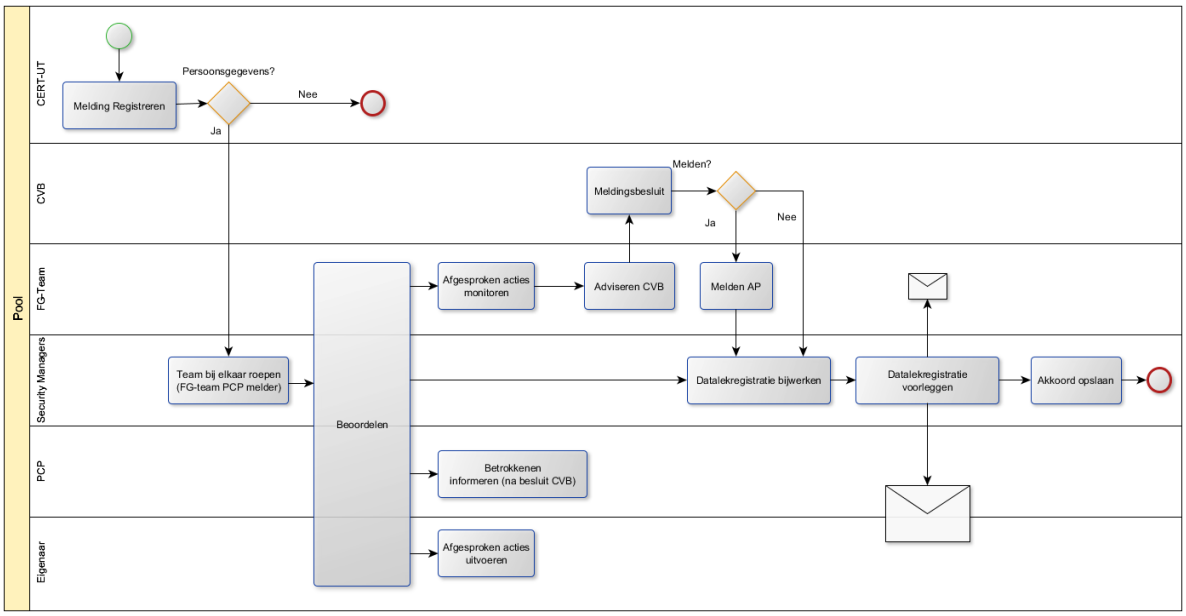
CERT-UT registers every report and, if necessary, contacts the employee who summited a report where additional information is required.

CERT-UT conducts an analysis and when it concerns personal data, it notifies the Security Manager (LISA), the Data Protection Officer (DPO, in Dutch FG: Functionaris Gegevensbescherming) and the Privacy Contact Person (PCP) of the unit.

The Security Manager is responsible for the handling of the data breach, for which evidence or information regarding the breach is stored in a safe environment. The Security Manager also handles the security incident underlying the data breach.

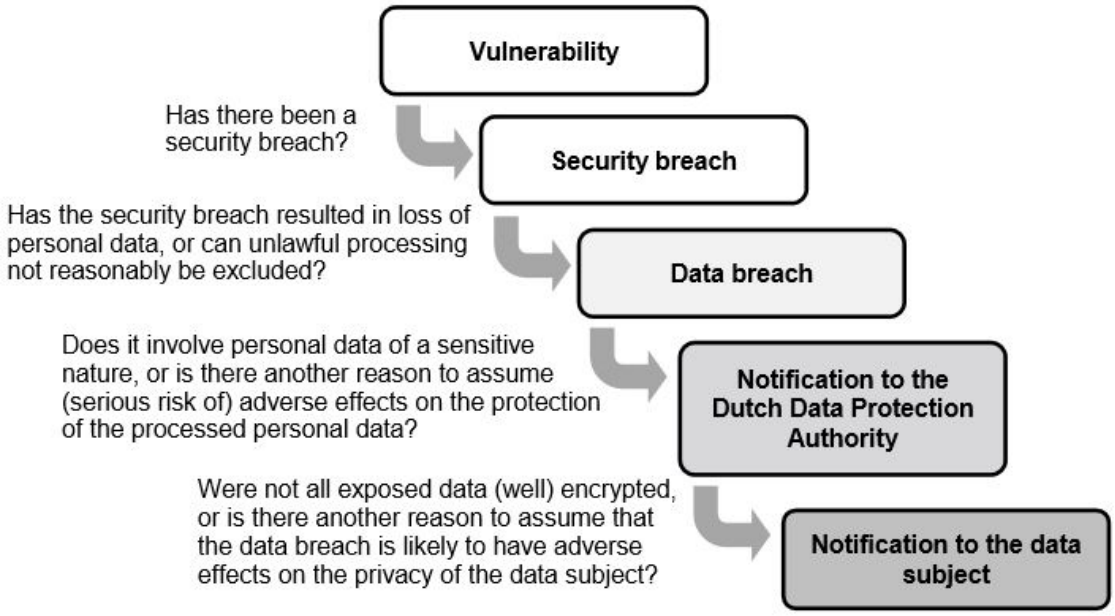
Together with a member of the DPO-team, the PCP of the faculty or service department concerned and the stakeholder of the incident, the Security Manager draws up a report. As part of this report, the Executive Board is advised whether or not to notify the Dutch Data Protection Authority (Dutch DPA) and the person concerned. A member of the DPO-team submits the advice to the member of the Executive Board responsible for business management.

Reports to the Dutch DPA are submitted by a member of the DPO-team, after consultation with the Executive Board. The PCP notifies the concerned parties. The Security Manager submits the report for approval to the PCP and to the person responsible for the data breach, via email. The report and approvals are archived in the register of data breaches by the Security Manager.



When to report?

For a detailed description of the assessment as to whether a report should be filed, see the Policy of the Dutch DPA. The diagram below illustrates the assessments.



Data breach
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.

Notification to the Dutch DPA
A security incident without a data breach does not need to be reported to the Dutch DPA. Similarly, not every data breach has to be reported. By law, you are required to notify the Dutch DPA if the data breach leads to a considerable likelihood of serious adverse effects on the protection of personal data.

Any information relating to an identified or identifiable natural person is personal data. This includes, for instance, names, addresses, licence numbers, phone numbers, IP-addresses, e-mail addresses, biometric characteristics, or a combination of specific preferences.

One factor that plays a role is the nature of the exposed personal data. If it concerns personal data of a sensitive nature, then a report is generally required. Potentially sensitive person data includes:

- Personal data about a person's religion or belief, race, political opinions, health, sexual life, membership of a trade union, as well as criminal personal data and personal data relating to unlawful or objectionable behaviour in connection with an imposed prohibition as a result of that.
- Data about the financial or economic situation of the data subject.
  This includes, for example, data on problematic debts, salary or payments details.
- Other data which may lead to stigmatization or exclusion of the person concerned.
  This includes, for example, data on gambling addictions, performances at school or at work or relational problems.
- User names, passwords and other login details.
  The possible impact on the data subjects will depend on the data processing and the nature of the personal data to which these login details give access. When assessing the impact one should consider that many people reuse passwords for different applications.
- Data which can be misused for identity fraud.
  This includes biometric data, copies of identity documents and the Citizen Service Number (CSN, in Dutch BSN).

Other factors, such as the amount of exposed personal data per person or the number of data subjects whose personal data have been affected, may be a reason to report the data breach. But beware: if the nature of the exposed data gives cause, it is possible that a data breach be reported where the personal data of only one person are involved.

The data breach needs to be reported without undue delay and if possible no later than 72 hours after the discovery 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. The law states that the person concerned must be notified if the data breach is likely to affect their privacy. The interests of those involved may be harmed by the loss, unlawful use or misuse of the data.

The law requires that the data breach be reported to the person concerned without delay, so that they can take measures to protect themselves against potential consequences of the data breach. The sooner the person concerned is informed, the sooner they can take action.

If appropriate technical protective measures have been taken, making the personal data concerned incomprehensible or inaccessible to unauthorized persons (e.g. encryption and hashing), then the data subject need not be notified. In this case, there will be no adverse consequences for the data subject.

Report
Quantitative reporting on data breaches is part of the quarterly security report prepared by the Security Manager (LISA).