UvA-AUAS Mandatory data breach notification

Since 25 May 2018, the (European) General Data Protection Regulation (GDPR) is in effect. This replaces the (Dutch) Personal Data Protection Act (Wbp).
The mandatory notification requires the UvA/AUAS to report data breaches to the Dutch Data Protection Authority (DPA) within 72 hours. Examples of data breaches are:

- The loss of a laptop or USB drive with research data of test subjects.
- A lost or stolen laptop/tablet with personal data of staff or students.
- Access to a UvAnetID or AUAS-ID containing personal data.
- Vulnerability in an Information System that allows unauthorized third parties to access personal data.

Certain criteria apply for an incident to be reported to the Dutch Data Protection Authority (DPA). Not all incidents need to be reported. CERT (see the UvA or the AUAS website for more information) will initially do research to determine whether the incident qualifies under the mandatory notification requirement. As part of their research, CERT may need to contact the reporter of the incident for additional information. Afterwards, the incident is submitted to the Data Protection Officer of the UvA/AUAS. The Data Protection Officer advises the Executive Board whether an incident needs to be reported to the Dutch data protection authority. The Executive Board ultimately decides if a notification is required. The Data Protection Officer also determines if the involved parties (the individuals whose personal data has been breached) need to be informed.

Contact details reporter incident:

Name:

Function:

Email address:

Phone number:

Details regarding the data breach:

Which equipment or system is involved in the data breach?

Please provide a summary of the incident in which the breach of personal data occurred:

How many individuals' personal data is involved in this data breach?

At least:

At most:

Describe the group of individuals whose personal data have been affected by this data breach:

When did this data breach take place?

Date:

Between and

Unknown:

What is the nature of the data breach? (multiple answers may apply)

- ☐ Reading (confidentiality)
- ☐ Copying
- ☐ Changing (integrity)
- ☐ Deleting or destroying
- ☐ Theft
- ☐ Not yet known
- ☐ Other:

What type of personal data is involved? (multiple answers may apply):)

- ☐ Name, address and residential data
- ☐ Phone numbers
- ☐ Email addresses or other addresses for electronic communication
- ☐ Access or Identification details (e.g., usernames and/or passwords)
- ☐ Financial details (e.g., bank account numbers or credit card numbers)
- ☐ Social Security Number
- ☐ Copies of passports or copies of other identity documents
- ☐ Sex, date of birth and/or age
- ☐ Special personal details (e.g., race, ethnicity, criminal details, political beliefs, membership union, religion, sexual activity, medical details)
- ☐ Other, namely:

Which effects can the data breach have on the personal lives of the involved parties?

- ☐ Stigmatization or exclusion
- ☐ Damage to health
- ☐ Subject to (identity) fraud
- ☐ Subject to spam or phishing
- ☐ Other, namely:

Which technical and/or organizational measures has your department taken to counteract the data breach and to prevent further data breaches?

Have the personal details been encrypted or in any other way been made incomprehensible or inaccessible for unauthorized parties?

- ◯ Yes
- ◯ No
- ◯ Partially, namely:

If the personal details have been made (partially) incomprehensible or inaccessible, in which way has this been done?

Does the data breach affect individuals in other countries of the EU?

- ◯ Yes
- ◯ No
- ◯ Not yet known