How is your data classified?

Having a dataset makes you a data controller. As a data controller, you are responsible for classifying your dataset and ensuring it is only processed in systems that are suitably secure.

If data is leaked, incorrect or vanishes, WUR may be impacted. The chance of this happening depends on the level of security measures that have been taken. The risk is the chance of an incident occurring in relation to the potential damage. WUR is willing to accept some risk, but not if the risk level is too high or if the risk is easily prevented. The higher the potential damage, the stricter the demands that apply to systems, thus mitigating the chance of an incident occurring.

The impact of a dataset is determined by the potential damage that may occur if the dataset’s availability, integrity or confidentiality is compromised. There are four classification categories: negligible, some, serious, and disruptive. The most severe impact is how the dataset is classified. The potential damage is assessed in four domains: operational, financial, reputation, and privacy.

Is the risk negligible? All systems are acceptable.

Is your system not listed? You can report the ApprovedApps procedure for your system. Need help? Contact your Information Security Officer.

Is your system not approved? Find an alternative system or dataset what additional security measures must be taken with your Information Security Officer.

**Classification category (Impact on WUR)**

- **Negligible**
  - No more than a single disruption of educational activity within a group. For example, a patient’s anonymized medical data.

- **Some**
  - A small portion of the data used is discontinued. For example, a dataset on summer vacations in the Netherlands, which includes information like name, age, gender, and location.

- **Serious**
  - A medium-sized disruption of educational activity in a group. For example, a dataset listing the names and telephone numbers of all students.

- **Disruptive**
  - A significant disruption of educational activity in a large group. For example, a dataset listing the names, addresses, and telephone numbers of all students.

**Operational Perspectives**

- **Negligible**
  - Disruption at a small part of an educational activity, such as administrative marks.

- **Some**
  - Disruption at a significant part of an educational activity, such as attendance records.

- **Serious**
  - Disruption at an important part of an educational activity, such as clinical records.

- **Disruptive**
  - Disruption at an essential part of an educational activity, such as examination questions.

**Financial Perspectives**

- **Negligible**
  - Losses of revenue, such as loss of revenue on research contracts, resulting from the leakage of data and the subsequent loss of potential revenue.

- **Some**
  - Losses of revenue, such as loss of revenue on research contracts, resulting from the leakage of data and the subsequent loss of potential revenue.

- **Serious**
  - Losses of revenue, such as loss of revenue on research contracts, resulting from the leakage of data and the subsequent loss of potential revenue.

- **Disruptive**
  - Losses of revenue, such as loss of revenue on research contracts, resulting from the leakage of data and the subsequent loss of potential revenue.

**Reputation Perspectives**

- **Negligible**
  - Negative posts in local websites and social media.

- **Some**
  - Negative posts in local websites and social media.

- **Serious**
  - Negative posts in local websites and social media.

- **Disruptive**
  - Negative posts in local websites and social media.

**Privacy Perspectives**

- **Negligible**
  - In cases where personal data are included in a dataset, the data must be classified as negligible.

- **Some**
  - A limited amount of personal data (≤100) may be sensitive in the context.

- **Serious**
  - A significant amount of personal data (100-1,000) may be sensitive in the context.

- **Disruptive**
  - A great amount of personal data (≥1,000) may be sensitive in the context.

**Questions?**

Contact your Information Security Officer or Privacy Officer.

**Is your data rated some, serious, or disruptive? Your data must be processed through a system from the ApprovedApps.**

**Is your system not listed? You can report the ApprovedApps procedure for your system. Need help? Contact your Information Security Officer.**

**Is your system not approved? Find an alternative system or dataset what additional security measures must be taken with your Information Security Officer.**