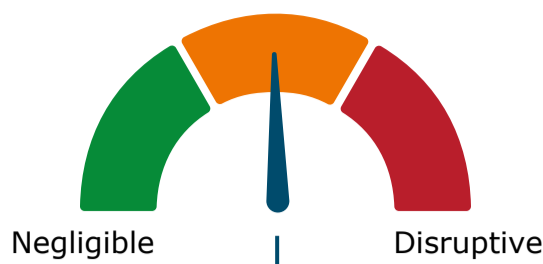# How is your data classified?

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.

Negligible — Disruptive

1 What impact would an incident have?

What would be the effect if the data were
- No longer accessible?
- No longer correct?
- Accessible to everyone?

Questions?
Contact your unit's Information Security Officer or Privacy Officer.

Classification category (Impact on WUR) → / Perspectives ↓	Negligible	Some	Serious	Disruptive
Operational	• No more than a single disruption of educational activity within a group. For example, a practical that cannot take place. This relates to, for example, digital tools needed for a practical. • No, or short interruptions of ongoing research or business. A copy of a dataset with non-confidential data, for example.	• Disruption of a small part of our education, such as one or more courses being interrupted. The learning materials of a single course, for example. • Interruption or rendering invalid of a single study, such as original research data used in only a small part of our research.	• Disruption of a significant part of our education affecting multiple groups and preventing them from teaching or administering exams. For example, the examination questions of a group. • Interruption of a significant number of research activities or disruption of the validation of many scientific studies. A dataset used in a significant number of studies, for example.	• Most education activities are rendered impossible for one or more units. For example, a dataset containing the results of all students. • Exclusion from future fundings or validation of a large number of studies is rendered impossible. For example, a dataset relevant to a large number of studies or essential in maintaining our leading position in the research domain. • Threats affecting (an) employee(s). For example, footage of identifiable researchers doing socially sensitive research.
Financial	• Loss of revenue, such as loss of research contracts, increased costs (for the renewed gathering of data) or fines (for a breach of contract) of less than €30,000. For example, a dataset that is used for a service with which WUR earns €10,000 euros annually.	• Loss of revenue, such as loss of research contracts, increased costs (for the renewed gathering of data) or fines (for a breach of contract) of between €30,000 and €300,000. For example, a dataset to which a research contract with a 40,000 euro penalty clause applies.	• Loss of revenue, such as loss of research contracts, increased costs (for the renewed gathering of data) or fines (for a breach of contract) between €300,000 and €3,000,000. For example, a dataset pertaining to a large, longitudinal study costing 400,000 euros.	• Loss of revenue, such as loss of research contracts, increased costs (for the renewed gathering of data) or fines (for a breach of contract) of over €3,000,000. For example, an ongoing patent application.
Reputation	• A small number of negative posts in local media/social media. For example, a discussion on intranet about paid parking on the campus.	• Negative posts in local media/social media over the period of several days. For example, raw data from an anonymous employee satisfaction survey.	• Negative articles in national media/social media for a short period. For example, controversial work, such as details on animal testing, which may be framed for publication.	• Persistent negative posts in national and international media/social media. Civic protests, both physical and digital. For example, studies on which (controversial) government policies are founded, such as data pertaining to nitrogen, for which data integrity has to be ensured.
Privacy	• In cases where personal details are included in a dataset, the risk can never be classified as negligible.	• A limited amount of personal data (<1000 individuals) or a small amount of personal data (<100 individuals) that may be sensitive within the context. For example, names, dates of birth, addresses and contact information. Financial information and social security numbers are examples of sensitive data.	• A more significant amount of regular personal data (>1000 individuals) or <1000 sensitive or <100 Special categories of personal data. Regular personal data includes names, dates of birth, addresses and contact information. Sensitive personal information includes financial information and social security numbers. Special categories of personal data includes information on ethnic background, medical information, and political or sexual orientation.	• A considerable amount of regular personal data (>10.000 individuals) or sensitive personal data (>1000 individuals), or Special categories of personal data (>100 individuals). Regular personal data includes names, dates of birth, addresses and contact information. Sensitive personal information includes financial information and social security numbers. Special categories of personal data includes information on ethnic background, medical information, and political or sexual orientation.

The aforementioned numbers are to be considered general guidelines rather than fixed limits.

Is the risk negligible? All systems are acceptable. ✓

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

2 Check whether the systems you are using are listed under ApprovedApps.

Check the ApprovedApps on the intranet.

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

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

WAGENINGEN
UNIVERSITY & RESEARCH