gesis Leibniz-Institut für Sozialwissenschaften

Licence compliance policy

External Document

07 December 2021
Version: 01.00

T +49 (0)221-47694-0
E deborah.wiltshire@gesis.org
www.gesis.org

gesis

Contents

Scope

This document outlines the policy for managing compliance with the terms and conditions of use of data services irrespective of access route for those data made available through the Secure Data Center at GESIS.

Definition of Terms

Commercial use of data

Research where a direct objective is to generate revenue and/or where data are requested for sale, resale, loan, transfer, or hire.

Controlled Data

Data which may be identifiable and thus disclosive or potentially disclosive and which can only be accessed via a secure data service.

Data Owner

The rights holder in any data collection.

Data Service

A service providing access to data for research purposes.

Data Use Agreement

The contract signed by a researcher. By signing this agreement, the data recipient agrees to terms and conditions of use associated with the Secure Data Center.

Data Recipient

A researcher registered with the Secure Data Center and who receives access to controlled data.

Non-compliance (incident or event)

A single action or series of actions by the data recipient that breaches the terms and conditions of the Data Use Agreement and any other procedure of the Secure Data Center.

Personal Information

Information that relates to and identifies an individual (including corporations) taking into account other information derived from published sources, made available under controlled access conditions via the Secure Data Center at GESIS.

1. Introduction

A researcher is required to apply to the Secure Data Center in order to access controlled data, agreeing to the Data Use Agreement. The Data Use Agreement applies to de-identified data which may pose a residual risk of data disclosure. The Data Use Agreement is designed to protect against unauthorised data disclosure by a data recipient.

A data recipient of disclosive data (which can only be accessed via the GESIS Secure Data Center) must sign a Data Use Agreement. The agreement includes:

- the purpose and period of usage;
- contract amendment policy;
- the data recipient's information security responsibilities;
- the non-compliances and penalties;
- data deletion policy where appropriate;
- acknowledgement and copyright requirements;
- warranty and liability of GESIS.

The agreement demonstrates that the data recipient understands the seriousness of the undertaking and that they understand the penalties that may be imposed for non-compliance with security or confidentiality or with the terms and conditions of access.

All GESIS staff are also required to sign a non-disclosure agreement that sets out their commitments.

Further, there is the potential for criminal penalties where there has been a non-compliance with the requirements of the relevant data protection legislation.

The Secure Data Center reserves the right to temporarily or permanently withdraw access to data and apply further penalties where it believes a data recipient is not in compliance, or does not intend to comply, with the terms and conditions of access to which the data recipient has agreed.

2. Events and incidents

Events and incidents will be handled in accordance with the Secure Data Center licence compliance procedures to ensure that:

- Data are protected.
- A proper investigation is undertaken.
- Appropriate records are kept.
- Effective action is taken.
- Communication is of an appropriate and effective nature.

The Data Use Agreement applies to data recipients of Controlled data. The majority of non-compliance incidents are procedural and can be handled without additional input from the data owner (although data owners will be notified of any non-compliances). However, more serious offences will be dealt with more strictly and could have serious consequences for the data recipient, including legal consequences.

3. Commercial use of data

Controlled access data are not available for commercial use at present.

4. Notification of publications

Under the Data Use Agreement data recipients are required to inform the Secure Data Center of any publications (e.g., external conferences, journal articles, reports). Whilst there is no formal penalty for failing to provide this information, as members of the research community data recipients are expected to share this information. Data recipients will be contacted from time to time to provide such information.

5. Right of appeal

The right to an internal appeal is allowed. The right of appeal is in the first instance to the Head of the Secure Data Center. However, the Head of the Secure Data Center will have no discretion to consider an appeal for a penalty or legal action applied by the data owner.

On appeal, a data recipient must show why the basis of the decision is wrong on factual grounds and/or why the penalty applied is disproportionate. The Head of the Secure Data Center has the discretion to remove, vary or increase any penalty already imposed.

Appendix A: Non-compliances and Penalties

GESIS is to be informed immediately in the event of any breach of the contractual obligations by the data recipient. The data recipient is liable for all damages to GESIS arising from actions not in accordance with this agreement, improper or incorrect handling in the context of access to the data made available whether via the data recipient themselves or the persons named on the Data Use Agreement and releases GESIS from any and all claims of liability or damages from third parties.

In this sense breach of contract includes, but is not limited to:

- Processing or usage of data for purposes other than the research project according to that given in the Data Use Agreement.
- No, or insufficient information regarding the source of data in publications.
- De-anonymizing or re-identification of individuals.
- Dissemination of data or data extracts to third parties.
- Unauthorized access to the data, even if this occurs via a lapse in IT security.
- Non-compliance with required standards for secure data storage and processing.
- Dissemination of personal access codes and passwords.

In the event of a breach of any of the obligations listed above GESIS may resort, depending upon circumstance and severity of the instance to one or more of the following measures:

- The data recipient will be required to immediately delete the database, including all backups, extract files and help files.
- An appropriate report on the breach will be sent to other research data and service centers and to the German Data Forum (*Rat für Sozial- und Wirtschaftsdaten*).
- The data recipient will at this time also be barred from access to services offered by GESIS for a limited time period.
- The data recipient will at this time also be permanently barred from access to services offered by GESIS.
- In the event of a willful, deliberate or grossly negligent breach of contractual obligations the data recipient agrees to the obligation of payment of a fine of €10,000 (Euro).

Factors to be taken into account when deciding which penalty is to be imposed:

- The application of any legislation, including the GDPR.
- This Licence Compliance policy

- Whether data was actually disclosed, and if so, what data (e.g. whole dataset, variable etc.).
- The disclosiveness and sensitivity of the data involved.
- To whom and how widely the data was disclosed.
- Whether the non-compliance was intentional.
- The data recipient's understanding of and acceptance of responsibility for the incident.
- Whether, given the information available to the individual, there should have been a clear understanding of the necessary licences and procedures, and the consequences of disclosure.
- Whether the data recipient has been involved in previous non-compliances.
- Penalties imposed in previous non-compliances with comparable circumstances.

Penalties may be imposed for any actions that do not comply with the Data Use Agreement. The penalties for non-compliances that are intentional and/or identified by the Secure Data Center or a third party will be dealt with more severely than non-compliances that are self-reported and unintentional. There is often no discretion in the imposition of penalties for intentional non-compliances. Data recipients who take full and prompt action to report and correct an unintentional non-compliance may receive lesser penalties but may be required to undergo training with the Secure Data Center before data access can be reinstated.

A non-compliance with procedures will be dealt with in the first instance by the Secure Data Center. Where the non-compliance relates to data legislation, the data service will assist the relevant data provider, should they wish to prosecute. A procedural non-compliance could occur that may or may not result in a criminal offence being committed, depending upon whether personal or confidential data is mishandled. For example, removing statistical outputs without the permission of the data service through any means is a non-compliance with procedures, but where this results in confidential data being removed from the Secure Data Center environment, then this may also be a legal breach.