Licence compliance policy

23 June 2022
Public

Version: 10.00

Table of contents

1. Scope

This document defines the policy for managing compliance with the terms and conditions of use for those data made available via UK Data Service labelled *Safeguarded* and/or *Controlled* irrespective of access route. Background information is provided concerning the agreements that Registered Users of the Service enter into and the legal framework that underpins those agreements.

2. Definition of terms

Registered User: A User who has registered with the UK Data Service and therefore agreed online to the End User Licence Agreement. Also referred to as the End User.

Authorised User: Member of an institution authorised by the UK Data Service to use the Data Collection(s) under a site licence or re-distribution agreement, or individuals who have signed an access agreement in relation to work being undertaken by a Registered User (e.g. students undertaking course-related work who have signed an Access Agreement for Teaching [Academic Sector] form).

ESRC Accredited Researcher: A Registered User to whom the UK Data Service and the data owner(s) have granted access to Controlled Data for the purposes of statistical research.

DEA Accredited Researcher: A User accredited under the Digital Economy Act 2017 (DEA) to access data for research purposes under the DEA and the Statistics and Registration Services Act 2007.

Data Service Provider: The person(s) or organisation(s) that directly provide the User with the Data Collections (on behalf of the Service Funder) and identified in the Metadata applicable to that Data Collection. A Data Service Provider may also provide user support, training, and research data management advice.

Service Funder: The persons or organisations that fund the Data Service Provider.

UK Data Service: Is a Data Service Provider funded by UKRI through the Economic and Social Research Council and supported by Universities of Essex, Manchester, Southampton, Edinburgh, University College London and Jisc. Also referred to as the Service. Also referred to as the Service.

User Agreement: An agreement setting out the terms and conditions of data use and establishing the rights and responsibilities of the Registered User.

End User Licence Agreement: The User Agreement entered into by a User when registering to access Safeguarded and Controlled data from the UK Data Service.

Special Licence User Agreement: The User Agreement entered into by a Registered User when using Safeguarded Data from the UK Data Service subject to additional data handling and storage conditions.

Secure Access User Agreement: The User Agreement entered into by a Registered User when using Controlled Data from the UK Data Service which are subject to Data Protection Legislation.

Data Protection Legislation: All applicable laws relating to data protection, the processing and use of personal data, including the General Data Protection Regulation, Regulation (EU) 2016/679 (GDPR), the UK General Data Protection Regulation (UK GDPR), Data Protection Act 2018 (DPA 2018), Digital Economy Act 2017 (DEA 2017), the Statistics and Registration Services Act 2007 (SRSA 2007), and any laws which replace, extend or amend any of the foregoing.

Commercial Use: Research is defined as 'commercial' where a direct objective is to generate revenue and/or where data are requested for sale, resale, loan, transfer or hire.

Non-Commercial Use: Any individual employed by, or undertaking research for any organisation, may use data even if this entails monetary reward, where a public good results from the use. Public good can be defined as an activity that widens access to information sourced from the UK Data Service collection and has social or economic benefits.

Safeguarded Data: UK Data Service Data Collections made available to Registered User(s) and where appropriate, additional conditions/agreements are agreed to.

Controlled Data: UK Data Service Data Collections made available to ESRC Accredited Researcher(s) and DEA Accredited Researcher(s) via the Five Safes Framework. Also referred to as Secure Access data.

Five Safes Framework: A set of principles which enables Data Service Providers to allow accredited researchers access to sensitive data or data classified as ‘Personal Data’ or ‘Personal Information’ consisting of five safes: Safe Data, Safe Projects, Safe People, Safe Settings and Safe Outputs.

Secure Researcher Training: Mandatory training provided to ESRC and DEA Accredited Researchers before they can access Controlled Data.

Personal Data: Are defined as in accordance with the UK General Data Protection Regulation (UK GDPR) Article 4(1) and the Data Protection Act (DPA) 2018 s3(2) as: data that relate to an identified or identifiable natural person, be it directly or indirectly, taking into account other information derived from published sources.

Personal Information: Information that relates to and identifies an individual (including a body corporate) taking into account other information derived from published sources (as defined in section 39(2) of the Statistics and Registration Service Act 2007).

Personal Data Breach: A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Information Security Event (Event): An identified occurrence of a system, service or network state indicating a possible breach of information security or failure of safeguards, or a previously unknown situation that may be security-relevant.

Information Security Incident (Incident): A single or series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.

Data Controller: The natural or legal person, public authority, agency or any other body which alone, or jointly with others, determines the purposes and means for the processing of Personal Data.

Depositor: The person named on the Deposit Licence Agreement having sufficient responsibility to grant particular rights on behalf of a Data Collection. The depositor may be the principal investigator, creator or the copyright owner of a Data Collection, or authorised to grant the Deposit Licence Agreement.

Deposit Licence Agreement: The non-exclusive agreement which entitles the UK Data Archive to include the Data Collection in its holdings and to provide access to the Data Collection under the conditions specified by the Depositor.

3. Background

A user is required to register with the UK Data Service in order to access Safeguarded or Controlled data, agreeing to the End User Licence (EUL) Agreement as part of their registration. The EUL applies to anonymised data that may pose a residual risk of data disclosure. The licence is designed to protect against unauthorised data disclosure by a user.

In addition to agreeing the EUL, some safeguarded data is subject to the Special Licence (SL) User Agreement.

In addition to the EUL, a user of Controlled Data, which can only be accessed via the UK Data Service SecureLab (SecureLab), must be either a “DEA Accredited Researcher” or an “ESRC Accredited Researcher” and must also sign a Secure Access User Agreement. The Secure Access User Agreement is countersigned by their institution’s authorised signatory such as the contracts office. The agreement includes:

- a requirement for the user to complete training
- the user’s information security responsibilities
- the non-compliances and penalties
- output release policy
- acknowledgement and copyright requirements.

The agreement demonstrates that the user understands the seriousness of the undertaking

and that they and their institution understand the penalties that may be imposed for non-compliance with security or confidentiality. Mandatory training (Secure Researcher Training) allows the UK Data Service to ensure that Accredited Researchers are fully aware of their commitments.

All Archive and Service staff are also required to agree the EUL and to sign a non-disclosure agreement which sets out their commitments.

Further, there is the potential for criminal penalties including a fine or imprisonment where there has been a non-compliance with Data Protection Legislation.

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

4. Events and incidents

Events and incidents will be handled in accordance with the *Managing 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.

4.1 Safeguarded data

Should any user commit a serious non-compliance with the terms and conditions of the End User Licence Agreement and/or Special Licence User Agreement if applicable, they may be subject to a suspension from access to any data available through these services and also to legal action being taken. As the severity of any non-compliance may vary, the response of the UK Data Service will vary.

The consequences of any suspension of access (such as an inability to honour research contracts) will not be taken into consideration when applying penalties.

4.2 Controlled data

The following agreements apply to users accessing Controlled data:

- End User Licence.
- Secure Access User Agreement.
- Any other official Agreement signed by the Accredited Researcher in order to access

Controlled Data.

A series of penalties for non-compliances will come into force at each level. The majority of these non-compliances are procedural and can be handled without additional input from the data owner (although data owners will be notified that a non-compliance has occurred*).* However, more serious offences will be dealt with more strictly and could have serious consequences for the user, including legal consequences.

5. Data Protection Legislation

Access to Controlled Data is regulated by Data Protection Legislation. Registered Users must accept their responsibilities relating to the use of Personal Data under the Data Protection Act 2018 and UK GDPR obligations or Personal Information under the section 39(2) of the Statistics and Registration Service Act 2007) before accessing the SecureLab.

Penalties under Data Protection Legislation include fine and/or imprisonment. For example, the SRSA 2007 states that a person who discloses Personal Information "is guilty of an offence and liable — (a) on conviction on indictment, to imprisonment for a term not exceeding two years, or to a fine, or both; (b) on summary conviction, to imprisonment for a term not exceeding twelve months, or to a fine not exceeding the statutory maximum, or both."[1]

Under the UK GDPR and DPA 2018 the maximum fine for data protection breaches is set to £17.5 million or 4% of annual global turnover, whichever is greater. This includes any Incident that affects the confidentiality, integrity or availability of personal data.[2]

The removal of Personal Information and/or Personal Data from the confines of the SecureLab is both an offence under Data Protection Legislation and a non-compliance with the Secure Access User Agreement (section 19). Users are informed in the training course that **only** statistical outputs, for publications, presentations, etc., which have been disclosure assessed and that they have received from a UK Data Service member of staff, can be released from the SecureLab environment.

SecureLab users of ONS Personal Information are made aware through training and service documentation that ONS has stated that it will always seek prosecution for any non-compliance with the SRSA 2007. The only exceptions are where the disclosure was unintentional and self-reported, or the 'reasonable belief' defence is unambiguous. Secure Researcher Training is designed to remove the ability to rely on the reasonable belief defence but non-compliances will still be open to judicial interpretation.

[1] Statistics and Registration Services Act 2007 § 39 (9).
[2] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/

6. Commercial use of data

Commercial Use of Safeguarded Data, if permitted, is specified by the data owners at the time of deposit. Controlled Data, regardless of their origin, are not available for Commercial Use.

7. Notification of publications, data errors and data enhancements

Registered Users are required to inform the UK Data Service of any publications (external conferences, journal articles, reports); any errors found in the data, or enhancements made to the data. Registered Users are regularly contacted to provide such information. In non-compliance events accounts are suspended. In addition all DEA Accredited Researcher must provide ONS with any final publications associated with the project they have been accredited for.[3]

8. Right of appeal

In the event of a penalty being applied for a breach of licence, Registered Users have a right to an internal appeal. This right of appeal is in the first instance to the Director, UK Data Service. However, the Director will have no discretion to consider an appeal for a penalty or legal action applied by the data owner.

On appeal, a Registered User must show why the basis of the decision is wrong on factual grounds and/or why the penalty applied is disproportionate. The Director has the discretion to remove, vary or increase any penalty already imposed.

3 https://www.ons.gov.uk/aboutus/whatwedo/statistics/requestingstatistics/approvedresearcherscheme

Appendix A: Non-compliances and Penalties

This Appendix sets out the likely consequences for users of failure to comply with a user agreement or any procedure prescribed by a data service, and the general principles underlying any decisions.

Types of non-compliance

- Procedural (e.g. not informing the UK Data Service of publications; sharing Safeguarded Data with unauthorised users.).
- Civil Offence (e.g. infringing UK Data Service's SecureLab security arrangements).
- Criminal Offence (e.g. sharing Controlled Data with unauthorised users).

Some types of non-compliance may fall under two headings depending upon the specific details.

In deciding a penalty regard will be had to:

- The application of Data Protection Legislation.
- This Licence Compliance Policy.
- What, if any, data was actually disclosed – its nature and volume (e.g., whole dataset, variable etc.).
- The disclosive nature and sensitivity of the data involved – whether held in SecureLab; subject to the Special Licence User Agreement; subject only to the End User Licence Agreement.
- The impact of the disclosure - to whom and how widely disclosed.
- Whether the non-compliance was intentional.
- The Registered User's understanding of and acceptance of responsibility for the incident.
- Whether, given the information available to the Registered User, there should have been a clear understanding of the necessary licences and procedures, and the consequences of disclosure.
- Other mitigating or extenuating circumstances presented by the Registered User, their senior colleagues or their institutions.
- Whether the Registered User has been involved in previous non-compliances.
- Penalties imposed in comparable situations.

The penalties for *intentional non-compliances identified by the service or a third party will be*

dealt with more severely than self-reported unintentional non-compliances. There is often no discretion in the imposition of penalties for intentional non-compliances. Registered Users who take full and prompt action to correct an unintentional non-compliance and who report the non-compliance may receive lesser penalties but may be required to undergo further training.

A non-compliance with procedures will be dealt with by the UK Data Service. Where the non-compliance relates to Data Protection Legislation, the UK Data Service will assist the relevant data owner, should the said organisation wish to make a prosecution. A procedural non-compliance could occur that may or may not result in a criminal offence being committed, depending upon whether Personal Information and/or Personal Data is mishandled. For example, removing statistical outputs without the permission of the UK Data Service is a non-compliance with procedures, but where this action results in Personal Information and/or Personal Data being removed from the SecureLab, then a criminal offence may have been committed.

Levels of penalty

In some cases there is little, if any, discretion about the penalty to be imposed.

- retraining
- temporary suspension from access to specific data and/or the UK Data Service
- permanent suspension from access to specific data and/or the UK Data Service
- removal of access to funding, e.g. by the ESRC
- civil proceedings
- criminal proceedings, which may lead to a fine or imprisonment.

Initial penalties

In the first instance, the following penalties will be applied based on the seriousness of the non-compliance:

Retraining (note this may be required whenever non-compliance is identified and in addition to any other penalty, unless a permanent ban on access to data is to be applied):

- 4 month suspension
- 6 month suspension
- 12 month suspension
- permanent ban on access to Controlled Data
- permanent ban on access to all UK Data Service data
- referral to the data depositor for consideration of further action; this may be in addition

to any of the above.

Table 1: General and Safeguarded Data Non-compliance Examples and Penalties

Non-compliance type	Non-compliance	Penalty	Primary responsibility for enforcement
Procedural	Not informing UK Data Service of publications	Suspension until remedial action under taken	UK Data Service
Civil Offence	Failure to report a non-compliance	Temporary or permanent suspension Possible legal action	UK Data Service/Depositor
Procedural **Civil Offence**	Using data for commercial purposes when not specifically permitted	Temporary or permanent suspension Depositor may impose additional penalties Possible legal action	UK Data Service/Depositor
Procedural **Civil Offence**	Incorrectly attributing copyright or other rights to oneself	Temporary or permanent suspension Depositor may impose additional penalties Possible legal action	UK Data Service/Depositor
Civil Offence	Transferring log in details to any other user	Temporary or permanent suspension Possible legal action	UK Data Service/Depositor
Civil Offence	Providing false information on, or altering, the Special Licence Agreement, Special Licence and Controlled Access Application Forms or SecureLab Access Agreement	Temporary or permanent suspension Possible legal action	UK Data Service/Depositor

Non-compliance type	Non-compliance	Penalty	Primary responsibility for enforcement
Civil Offence **Criminal Offence**	Attempt to access datasets to which not authorised and/or to use data for purpose not specified in the application	Temporary or permanent suspension Possible legal action	UK Data Service/Depositor
Civil Offence/ Criminal Offence	Attempt to identify respondents	Expected Penalty a) Permanent suspension from all ESRC data services (individual); AND b) 1 year suspension from all ESRC data services (institution) AND c) permanent sanction from ESRC funding (individual) AND d) 5 year sanction from ESRC funding (institution) Possible legal action	ESRC/UK Data Service/Depositor
Procedural **Civil Offence**	Sharing Safeguarded Data with non-authorised users	Temporary or permanent suspension Possible legal action	UK Data Service/Depositor
Procedural	Not following guidance on outputs that can be published using data subject to the Special Licence Agreement	Temporary or permanent suspension	UK Data Service/Depositor

Table 2: Controlled Data Non-compliance Examples and Penalties

Non-compliance type	Non-compliance	Penalty	Primary responsibility for enforcement
Procedural	Applying for Accredited Researcher status without intent to use data	Temporary or permanent ban on making Accredited Researcher applications	UK Data Service/Depositor/Data Controller
Procedural	Access to Controlled Data from an inappropriate environment or place	Notification to listed data services. Temporary or permanent (i) suspension from listed data services (ii) sanction from listed funders.	UK Data Service/Depositor/ Data Controller/ESRC
Procedural	Use of prohibited items in a secure room	Notification to listed data services. Temporary or permanent (i) suspension from listed data services (ii) sanction from listed funders.	UK Data Service/Depositor/ Data Controller/ESRC
Procedural	Copying statistical information or data from the screen when accessing Controlled Data	Notification to listed data services. Temporary or permanent (i) suspension from listed data services (ii) sanction from listed funders.	UK Data Service/Depositor/ Data Controller/ESRC
Civil Offence/Criminal Offence	Sharing any outputs from Controlled Data which have not been approved	Temporary or permanent suspension Possible legal action NB sharing data outputs which prove to be disclosive will be subject to more severe penalties.	UK Data Service/Depositor/Data Controller

Non-compliance type	Non-compliance	Penalty	Primary responsibility for enforcement
Procedural/Civil Offence	Infringing SecureLab security requirements	Expected Penalty a) Temporary or permanent suspension (individual); AND b) 1 year suspension (institution) AND c) Up to 5 year sanction from ESRC funding (individual) AND d) 1 year sanction from ESRC funding (institution) Possible legal action	ESRC/UK Data Service/Depositor/Data Controller

Non-compliance type	Non-compliance	Penalty	Primary responsibility for enforcement
Civil Offence/ Criminal Offence	Sharing Controlled Data with unauthorised users	Expected Penalty a) Permanent suspension from all ESRC data services (individual); AND b) 5 year suspension from all ESRC data services (institution) AND c) permanent sanction from ESRC funding (individual) AND d) 5 year sanction from ESRC funding (institution) Possible legal action Making Personal Information available to others is a criminal offence and non-compliances may be subject to prosecution at the discretion of ONS. Identifying an ONS respondent and providing that detail to another party for personal gain is a serious criminal offence in the Statistics and Registration Service Act, with potentially a 2 year jail term, a £2000 fine, and a criminal record. Making Personal Data available to others is a criminal offence and may be subject to prosecution in accordance to Data Protection Legislation at the discretion of the ESRC and the data depositor.	UK Data Service/Depositor/Data Controller/ESRC

www.ukdataservice.ac.uk

collections@ukdataservice.ac.uk

We are supported by the Universities of Essex, Manchester, Southampton, Edinburgh, University College London and Jisc. We are funded by UKRI through the Economic and Social Research Council.