UK Data Service

Licence Compliance Policy

External

03 AUGUST 2017
Version: 09.00

T +44 (0)1206 872001
E wardm@essex.ac.uk
www.ukdataservice.ac.uk

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 labelled safeguarded and/or controlled. Background information is provided concerning the agreements that users of the service enter into and the legal framework that underpins those agreements.

Definition of Terms

Commercial use of data

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, see: http://ukdataservice.ac.uk/get-data/how-to-access/registration/commercialusers.aspx

Controlled Data

Data which may be identifiable and thus disclosive or potentially disclosive.

Data Owner

The rights holder in any data collection

Data service

A provider of access to data for a user.

Declaration

The declaration signed by a researcher in the ONS Approved Researcher, or ESRC Accredited Researcher application. Briefly, the researcher declares that they understand the terms and conditions of the licence under which they apply for access.

Depositor

A depositor is an individual who is named on a Licence Agreement as having sufficient responsibility to grant particular rights to the UK Data Archive on behalf of a data collection. The depositor may be the instigator, creator or the copyright owner of a data collection, but does not have to be. In OAIS terminology the term producer is used in a similar sense.

End User Licence (EUL)

The user agreement entered into by a user when registering to access data from the UK Data Service (see *End User Licence)*. Users who access data via the Secure Lab necessarily agree to the EUL as they must register with the UK Data Service during the process of applying for access.

ESRC Accredited Researcher (AR)

A user to whom the UK Data Service and the data owner(s) have granted access for the purposes of statistical research to Personal Information not held by the UK Statistics Authority and which have been licensed to the UK Data Archive/University of Essex for dissemination.

Higher Education (HE) users

Users who are employed or study at a UK Higher Education Institution (for example, a university).

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.

Non-Higher Education (non-HE) users

Users who are granted access to data via the Secure Lab but who are not employed (or study) at a university; Instead, they are employed at an ESRC-funded Research Institute (for example, the Institute for Fiscal Studies).

ONS Approved Researcher (AR)

A user to whom the UK Statistics Authority, under the Statistics and Registration Services Act (SRSA) 2007, has granted access to Personal Information held by it for the purposes of statistical research.

Personal Information

Information that relates to and identifies an individual (including a body corporate) taking into account other information derived from published sources, made available under controlled access conditions via the UK Data Service Secure Lab.

Safeguarded Data

Data licenced for use in this category are not personal, but the data owner considers there to be a risk of disclosure resulting from linkage to other data, such as private databases.

Secure Access User Agreement

The agreement signed by a user (and by a representative of their institution). By signing this agreement, the user agrees to terms and conditions of use associated with the Secure Lab, and additional to those of the EUL and the Declaration.

Special Licence (SL)

A licence additional to the EUL for certain safeguarded data that need additional protection.

User

An individual registered with the UK Data Service.

User Agreement

An agreement setting out the terms and conditions of use of a data service and establishing the rights and responsibilities of the user of that service.

1. Introduction

A user of a data service is required to register with the UK Data Service in order to access safeguarded or controlled data, agreeing to the End User Licence (EUL). The EUL applies to anonymised data which 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 also require the user to agree a Special Licence (SL).

In addition to the EUL, a user of controlled data (which can only be accessed via the UK Data Service Secure Lab (Secure Lab)) must be either an “ONS Approved Researcher” or an “ESRC Accredited Researcher” (AR) and must also sign a Secure Access User Agreement which is countersigned by their institution’s contracts office. The agreement includes:

- a requirement for the user to complete Safe User of Research Data Environments (SURE) 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 SURE training allows the UK Data Service to ensure that ARs are fully aware of their commitments.

All Archive 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 where there has been a non-compliance with the requirements of the Statistics and Registration Services Act.

The 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.

2. 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

2.1. Safeguarded data

Should any user commit a serious non-compliance with the terms and conditions of the EUL or a SL, 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 Archive’s response will vary.

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

2.2. Controlled data

The following agreements apply to users of Controlled data and can be characterised as an order of incremental gravity in the event of a non-compliance:

- End User Licence;
- Special Licence;
- Approved/Accredited Researcher declaration;

- Secure Access User Agreement.

A series of penalties for non-compliances additional to those of the EUL 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.

3. The Statistics and Registration Service Act 2007 (SRSA)

The SRSA 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]

The removal of Personal Information from the confines of the Secure Lab is both an offence under the SRSA and a non-compliance with the Secure Access User Agreement (section 19). Users are informed in the training course that **only** statistical outputs (publications, presentations, etc.) which they have received from a UK Data Service member of staff, are non-disclosive.

Secure Lab 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. SURE training is designed to remove the ability to rely on the reasonable belief defence but non-compliances will still be open to judicial interpretation.

4. Commercial use of data

Whether commercial use of Controlled or Safeguarded data is permitted, and under what circumstances, is specified by the data owners at the time of deposit. Controlled access data, regardless of their origin, are not available for commercial use at present.

5. Notification of publications, data errors and data enhancements

Under user agreements users are required to inform the data service of any publications (external conferences, journal articles, reports); any errors found in the data, or enhancements made to the data. Whilst there is no formal penalty for failing to provide this information, as members of the research community users are expected to share this information. Users will be regularly contacted to provide such information.

6. Right of appeal

The right to an internal appeal is allowed. The 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 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.

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.

In deciding a penalty regard will be had to:

[1] Statistics and Registration Services Act 2007 § 39 (9).

- The application of any legislation, including the SRSA.
- 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 Secure Lab; subject to Special Licence; subject only to the End User Licence.
- The impact of the disclosure - to whom and how widely disclosed.
- Whether the non-compliance was intentional.
- The user'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.
- Other mitigating or extenuating circumstances presented by the user, their senior colleagues or their institutions, such as the impact of the penalty on the researcher's involvement in any given piece of research.
- Whether the individual 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. 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.

Penalties may be imposed for any offences that constitute non-compliance with a user agreement.

It should be noted that whilst survey respondents are not the owners of the data for the purposes of this document, they have the right to take independent civil action against any offender who damages them by release of their Personal Information.

A non-compliance with procedures will be dealt with by the data service. Where the non-compliance relates to data legislation, the 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 or confidential data is mishandled. For example, removing statistical outputs without the permission of the data service is a non-compliance with procedures, but where this action results in confidential data being removed from the Secure Lab, then a criminal offence may have been committed.

Types of non-compliance

- Procedural (e.g. not informing the Data Service of publications)
- Civil Offence (e.g. infringing Secure Lab 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.

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 Data Service.
- Permanent suspension from access to specific data and/or the 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 tariff of penalties will be applied based on the seriousness of the non-compliance:

- Retraining. 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 Secure Lab data.
- Permanent ban on access to all data.
- Referral to the data depositor for consideration of further action. This may be in addition to any of the above.

Table 1: Sample Range of Non-compliances and Penalties

Non-compliance	Penalty	Primary responsibility for enforcement	Type
Not informing UK Data Service of publications	Suspension until remedial action under taken	UK Data Service	Procedural
Sharing safeguarded data with non-authorised users	Temporary or permanent suspension Possible legal action	UK Data Service/Depositor	Procedural Civil Offence
Failure to report a non-compliance	Temporary or permanent suspension Possible legal action	UK Data Service/Depositor	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
Not following guidance on outputs that can be published using SL data	Temporary or permanent suspension	UK Data Service/Depositor	Procedural
Applying for AR status without intent	Temporary or permanent ban on making AR applications	UK Data Service/Depositor	Procedural

to use data			
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/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/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/ESRC	Procedural
Incorrectly attributing copyright or other rights to oneself	Temporary or permanent suspension. Depositor may impose additional penalties. Possible legal action	UK Data Service/Depositor	Procedural 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 SL, AR Form, Declaration or Secure Lab Access agreement	Temporary or permanent suspension Possible legal action	UK Data Service/Depositor	Civil 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
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	Civil Offence / Criminal Offence
Infringing Secure Lab 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	Procedural Civil Offence
Attempt to identify respondents	*Expected Penalty* a) Permanent suspension from all ESRC data services (individual); AND	ESRC/UK Data Service/Depositor/ESRC	Civil Offence/ Criminal Offence

	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 For ONS Approved Researchers attempting to re-identify respondents is a criminal offence, and non-compliances may be subject to prosecution at the discretion of ONS.		
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 disclosive ONS data 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 non-ONS disclosive data available to others is a criminal offence and may be subject to prosecution at the discretion of the ESRC and the data depositor.	UK Data Service/Depositor/ESRC	Civil Offence/ Criminal Offence