Restricted Data Policy

Policy Number: PP15
5th May 2015

Introduction

DRI advocates for data ingested into the Repository to be made publicly accessible on the web. DRI also encourages the application of Creative Commons licences to data where possible, allowing digital objects to be reused for certain purposes which have been approved by the copyright owner. In relation to data which has been generated by public bodies or in the course of publicly-funded research, DRI supports the principles of Open Access, which state that such data should be made openly available for use and reuse as long as the creator is properly acknowledged and cited (see DRI position statement on Open Access).

For some categories of data the implementation of appropriate controls is required. This is particularly the case where it is necessary to protect the privacy of individuals and organisations and to ensure that sharing research outputs meets internationally recognised professional ethical standards and conforms to national and European law. Moreover, there may be circumstances where there is court-ordered disclosure of data, and in those circumstances, it may not be possible to respect the confidentiality of data or to protect the privacy of individuals and organisations.

This document describes DRI's approach to implementing restrictions on data deposit and dissemination. It also outlines the DRI response to requests, demands or court orders for disclosure of restricted data or for the data to be removed from public access.
DRI respects the core principles of ethical research in the humanities and social sciences, namely:

- 'do no harm',

- informed consent,
- protection of anonymity,
- Compliance with the law of the land, particularly in terms of data protection and privacy

In addition, DRI subscribes to the RESPECT Code of Practice recommendation that:

> In general, socio-economic researchers should comply with the laws of the country in which they are based or in which they are carrying out research. In the case of international collaborations or online research, the laws of additional countries may also apply. Researchers have a duty to ensure that their work complies with any relevant legislation. Two areas of law (data protection law and intellectual property law) are particularly relevant for the conduct of research, especially research involving human subjects, and researchers should acquaint themselves with the relevant national and international provisions.(RESPECT 2004)

DRI recognizes that under exceptional circumstances professional research ethics may come into conflict with the law, especially where the law may compel disclosure. This document describes how DRI will meet its legal obligations in these circumstances (a Law of the Land position) while advocating for an 'ethics first' position [1].

Access Control

DRI supports a range of access controls to data. These are outlined below.
All users are prompted agree [via a tick box] with the standard end user agreement.

[1] Palys & Lowman (2012) outline two approaches to research confidentiality; the Law of the Land Position and the 'ethics first' position: "If .. lawful attempts to defend research confidentiality fail, and the researcher is ordered to disclose confidential

Publicly access data/ unrestricted data: applies to all our metadata (and can also apply to objects and collections). Users are prompted to agree [via a tick box] with the standard end user agreement. Registration is not required. Unregistered users are able to view the data.

Restricted data:

In order to safeguard certain kinds of data, especially those generated through research carried out with human subjects, DRI will allow for the imposition of two different types of data restriction. We will follow these definitions

Safeguarded data:

Safeguarded data*/* ***Standard access***: Users are prompted to agree [via a tick box] with the standard end user agreement. Registration is required in order to be able to view the data.

Safeguarded Data*/* ***Special Conditions***: Some data collections are subject to additional conditions of access. Users are prompted to agree [via a tick box] with the standard end user agreement. Registration is required in order to be able to view the data. Users will have to meet further special conditions. These special conditions include one and/or more of

- The user must wait until an embargo period has expired, ie data only available after a time period.
- The user has registered with an edugate account
- The user completes a *Special Condition Data Access* form.
- Additional special conditions: the user must be manually approved by the depositor who will ensure that the user meets the additional special conditions.

DRI Ethical Principals (Restricted Data)

1. DRI will clearly inform researchers of the repository's ethical position and legal obligations relating to restricting access to data or to disclosing data.

    DRI will take **all reasonable and lawful** steps to ensure that the permissions granted by the depositor will be enforced by the system. [note: this is currently in the Organisational Managers agreement]

DRI will not unlawfully delete or restrict access to data. We outline how DRI will respond to court orders for disclosure of data in point 4 below.

2. DRI will clearly inform the depositor that it will not necessarily delete restricted data on request of depositor.

In general, the Repository will decide whether or not an object will be stored or retained in or removed from the system, or made available to the public. As a consequence, the withdrawal, removal or deletion of digital objects or metadata from the Repository is a matter for the Repository and will only happen in exceptional circumstances. Where this occurs, pursuant to a request in writing from an Organisational manager, there is likely to be a charge to cover the cost of this service. If requested in writing by the Organisation Manager, the Repository will return the original digital object to the Organisational Manager.

3. DRI will notify the Organisational Manager of any threat to the collection.

DRI will promptly notify the Organisational Manager and Depositor of any copyright, confidentiality, privacy, data protection, defamation, or similar or related issues, raised by third parties, pertaining to the digital objects.
DRI will promptly notify the Organisational Manager and Depositor if required to edit access permission where any such issue has arisen.
DRI will act promptly in association with the Organisational Manager and Depositor to ensure that the most appropriate action is taken, including but not limited to actions pursuant to any applicable notice and action procedure.

4. DRI will outline any response to requests, demands or court orders for disclosure of restricted data or for the data to be removed from public access. Similarly in cases where notice and action procedures are exhausted or inappropriate, DRI will outline any response to a demand, request or court order.

4.1 Any such demand, request or court order should be referred immediately to the Director of DRI.

4.2 If necessary, the Director of DRI, working with the Organisational Manager involved, will seek legal advice to establish the lawful authority of the demand, request or court order.

4.3 In the case of demands or requests, the Director of DRI will seek to negotiate with the requesting body to attempt to agree on an acceptable course of action, especially those that would protect the confidentiality of the data and the participants.

4.4 If it is not possible appropriately to protect the confidentiality of the data and the participants by negotiation and agreement, then DRI will consider what other steps to take, including making an application to an appropriate court to protect the confidentiality of the data and the participants.

4.5 In the case of a court order, DRI will consider a further application to an appropriate court to protect the confidentiality of the data and the participants.

4.6 DRI will abide by the court's decision, subject to any appeal mechanisms which it may be feasible and reasonable to pursue.

4.7. Every effort will be made to ensure that, if confidential non-anonymised data must be released, then, in so far as possible, any person to whom a commitment of confidentiality has been made will be informed prior to the data being released to an outside agency or person.

4.8 DRI will make public the legal threat to the confidentiality of the data, unless precluded from doing so by court order.

5. DRI will advocate for Academic Privilege[2] for Researchers.

6. DRI will advocate on behalf of archival staff who adopt an 'ethics first' consent, that is who refuse to enable access to data which would be in contravention of a depositor's wishes.

[2] "The academic's privilege is one variant of the reporter's privilege, which has long been advanced to excuse journalists from disclosing the identities of their confidential sources". Havemann, W (2012) Stanford Law Review Online, 79 p79, Also Robert M. O'Neil, A Researcher's Privilege: Does Any Hope Remain?, 59 LAW & CONTEMP . PROBS. 35, 37, 44 (1996).

CONSENT

Depositors must ensure that data generated through research with human subjects has been processed with due consideration for the core ethical principles outlined in the introduction to this document (and elaborated in national, European and international codes of research ethics. See Annex 10.2, DASISH D6.1). In most cases, DRI will only ingest data generated through research with human subjects where participants have provided informed consent for sharing and re-use.

The Organisational Manager and Depositors must sure that the consents collected are appropriate and sufficient to allow deposit within DRI. In particular, the Organisational Manager and Depositors **must not** deposit un-anonymised data collected under consents which promise to protect confidentiality without recognizing legal limitations on such promises of confidentiality.

.

ANONYMISATION

Where data has been generated through research with human subjects, adherence to professional ethical standards and/or compliance with legal obligations may require that data be anonymised. In particular, personal or organizational identifiers may be removed or disguised, or in some cases that the data must be selectively altered, in order to ensure that individuals, organizations or places cannot be identified. Anonymisation may not be required, for example, in oral histories or in anthropological research, where it is customary to publish and share the names of people interviewed provided that they have given their consent.

DRI recognizes that anonymisation may have deleterious consequences for the integrity and authenticity of data. However, even when informed consent has been obtained, depositors must take due account of the potential ethical and legal consequences of depositing un-anonymized data. **In particular, they must not rely on the restrictions on access provided for under DRI's special conditions, to secure the privacy and well-being of participants.** Depositors should therefore be aware that there is a risk of legally-mandated disclosure attached to depositing data (even if deposited as a restricted data set).

Depositors should ensure that they have anonymised the data appropriately and sufficiently and should consult best practice guides on anonymisation (such as that

produced by the Irish Qualitative Data Archive[3])

[3] http://www.iqda.ie/sites/default/files/AnonymisationProtocolV5.pdf Accessed 16th June 2015