



A joint Research Councils Programme co-sponsored by Defra and SEERAD

Data resources for rural sustainability research: realising their combined potential.

Annex B

Review of legislation relevant to the RELU programme

Helen M^cKay, Central Science Laboratory, Sand Hutton, York YO41 1LZ, U.K.
h.mckay@csl.gov.uk

29 June, 2005.

Annex B. Review of legislation

Contents

Executive Summary	1
Introduction.....	2
Methods.....	2
Review	3
Freedom of Information Act 2000 (FOIA)	3
Data Protection Act 1998 (DPA)	4
Environmental Information Regulation 1992: 1998 (EIR).....	5
Re-use of Public Sector Information Regulations	7
Privacy and Electronic Communications (EC Directive) Regulations 2003	7
The Copyright and Rights in Databases Regulations 1997	8
Intellectual Property.....	9
Public Service Guarantee on Data Handling	9
Competition Act 1998.....	10
The Human Rights Act 1998	10

Executive Summary

1. This review aims to provide land use and rural economy researchers with information on current legislation relevant to data access and sharing. This review is our interpretation. Although every effort has been made to verify accuracy, the sources used are given in the Methods section, so that researchers can check for themselves.
2. In the UK, it is the Information Commissioner's responsibility to promote good information control practice and enforce information control legislation.
<http://www.informationcommissioner.gov.uk/eventual.aspx>
3. The **Freedom of Information Act 2000** gives the public the general right to see recorded information held by public authorities. Both Environmental and Personal information are exempt, as they are covered by other legislation. The relevance to RELU is that researchers can: (a) request data held by public authorities, and (b) expect information on data holdings to exist. Requests for information must be communicated if the information exists and if it does not fall within an exemption category; Commercial/In Confidence-labelled information is not exempt.
4. The **Data Protection Act 1998** sets out the terms and conditions under which personal data will be processed. It covers all personal records and data held in paper and electronic systems and provides a right of access to the public. Sharing personal data is unlawful if it would breach confidence or break a law.
5. The **Environmental Information Regulations 1992: 1998** establish an access regime that allows people to request environmental information from public authorities and those bodies carrying out a public function Confidentiality clauses do not generally prevent disclosure or sharing of data and there are no other restrictions on data sharing imposed by the EIR.
6. Other Regulations and Acts are briefly reviewed (Privacy And Electronic Communications (EC Directive) Regulations 2003, The Copyright and Rights in Databases Regulations 1997, Public Service Guarantee On Data Handling, Competition Act 1998, The Human Rights Act 1998 and The Regulatory Reform Act 2001).
7. Information not held by public bodies is subject to intellectual property rights, and may be protected by copyright or other IP laws.

Introduction

The RELU programme takes an integrated, interdisciplinary approach to research on rural issues. Researchers therefore require access to a wide range of data and computational tools to carry out integrated analyses. Legislation exists in order to ensure public access to data, protect personal data and protect commercial interests. These regulations may have an impact on the way data is shared within the RELU programme.

This review aims to provide land use and rural economy researchers with relevant information on current legislation.

Methods

The following sources of information were used:

- the UK Freedom of Information Act Blog website:
http://foia.blogspot.com/archives/2004_01_01_foia_archive.html
- the UK Information Commissioner's website:
<http://www.informationcommissioner.gov.uk/>
- the Davenport Lyons Legal Services website:
http://www.davenportlyons.com/www/legal_services/it_and_new_media/articles/pdfs/Special_Release_Copyright_and_Rights_in_Database_Regs.pdf
- the UK government sustainable development website:
http://www.sustainable-development.gov.uk/what_is_sd/transparency.htm
- Defra environmental protection website:
<http://www.defra.gov.uk/environment/pubaccess/guidance/01.htm>
- New UK Environmental Information Regulations (on the Defra website):
www.defra.gov.uk/corporate/consult/envinfo/index.htm.
- IGGI (Intra-government Group on Geographic Information) Guide: Principles and practice of sharing and trading Government Information. 2001.
www.iggi.gov.uk/publications/index.htm
- The Government-backed home of UK Intellectual Property on the Internet.
<http://www.intellectual-property.gov.uk/>

Annex B. Review of legislation

Review

In the UK, it is the Information Commissioner's responsibility to promote good information control practice and enforce information control legislation (the Freedom of Information Act 2000, the Data Protection Act 1998 and the Environmental Information Regulations 2004 and the Privacy and Electronic Communications Regulations 2003).

FREEDOM OF INFORMATION ACT 2000 (FOIA)

FOIA is a law giving the public the general right to see recorded information held by public authorities. Both Environmental and Personal information are exempt, as they are covered by other legislation. The relevance to RELU is that researchers can: (a) request data held by public authorities, and (b) expect information on data holdings to exist. Requests for information must be communicated if the information exists and if it doesn't fall within an exemption category; Commercial/In Confidence-labelled information is not exempt.

The FOIA covers all public bodies, from central government departments to local authorities, to schools and doctors' surgeries (termed the *public authority*). It came into force on 1 January 2005 (replacing the Code of Practice on Access to Government Information).

There are three main features of the FOIA: access rights, publication schemes and records management requirements.

Under this Act, any member of the public, from any country, and for any reason, can request information, for any purpose, in writing (includes e-mail), and this must be actioned within 20 working days of receipt. The requester must state the name and address of the person applying, and the required information. The requester must be told whether the specified information is held and if that is the case, that information must be communicated unless it falls within an exemption category. The applicant can either ask for a copy of the information, to inspect the records, or to be given a summary of the information, and the public authority must try to provide the information in this form. Public authorities are allowed to charge a set fee, for providing the information.

The exemption covers personal data about the requester (as that is covered by the DPA), environmental data (as that is covered by the EIR) and personal data about someone else (termed *third party data*) if disclosure should breach any of the eight Data Protection Principles (listed in the DPA section). In relation to third party data, disclosure would be unlawful (the first principle of the DPA) if there would be a breach of confidence or if there is a law forbidding disclosure (e.g. Official Secrets Act and the Animals (Scientific Procedures) Act 1986). Also under the first principle is fairness. Generally it is unfair to disclose personal information on the *private* lives of individuals. Where information is requested about people acting in a work or official capacity then normally disclosure would be lawful.

FOIA is fully retrospective and covers all information including that which is protectively marked or confidential.

Subject access requests must be made in writing (includes e-mail). Requesters' identity should rarely need verified (in contrast to the DPA).

Annex B. Review of legislation

Under the FOIA, public authorities must produce a Publication Scheme, giving details of what information it already makes available or intends to publish as a matter of course. FOIA also introduces new standards for records management.

DATA PROTECTION ACT 1998 (DPA)

The DPA sets out the terms and conditions under which personal data will be processed. It covers all personal records and data held in paper and electronic systems and provides a right of access to the public. Sharing personal data is unlawful if it would breach confidence or break a law.

This Act sets out the terms and conditions under which personal data (i.e. information relating to living individuals, from which the individual can be identified) will be processed. If data have been stripped of all personal identifiers, and the original data (from which individuals could be identified) destroyed, the data cease to be personal data and are not covered by the DPA. Processing means obtaining, recording or holding the information or data or carrying out any operation on the data (which includes organisation, use, disclosure or destruction).

The DPA is not restricted to information held by/on behalf of public authorities, nor is its purpose limited to the right of access to information. The Act covers all personal records and data held in paper and electronic systems. The DPA provides a right of access to the public regarding personal data as long as they are themselves the subject of the data – this is called the right of subject access. Subject access rights include:

- A copy of the data of which they are the subject
- Information about the purpose of the data
- Who has access to the data
- The source of the information

All personal data must be processed in accordance with the Eight Data Protection Principles; data must be:

1. Processed fairly and lawfully
2. Processed for specific purposes
3. Adequate, relevant and not excessive
4. Accurate and up to date
5. Kept for no longer than necessary
6. Processed in accordance with the rights of the data subject
7. Kept secure
8. Data must only be transferred outside the European Economic Area if there is adequate protection

In relation to the first principle, disclosure would be unlawful if there would be a breach of confidence, or if there is a law forbidding it. The law of confidence is a common law concept (i.e. developed by the courts as individual cases have been brought before them). The key issue is likely to be the circumstances under which information was provided, essentially, that conditions (explicit or implied) were attached to its subsequent use or disclosure. ‘Implied conditions’ may give rise to some uncertainty, if the expectations of the confider and confidant are different. The issue of relevance here seems to be that if data collected by a public body are to be shared, the intention to do so must be made explicit (and not just implied or assumed)

Annex B. Review of legislation

when the data are collected, in order to avoid legal action. This includes data collected under statutory obligation. This is the advice that was given to Defra Geographical Information Unit, that is, that the DPA does not prevent data sharing (Bill Froggatt, pers. comm., Defra GIU). Another relevant point is that if data are shared with a third party, and a request for access to this information is made to the third party under the DPA, the information must be disclosed even if a contract exists restricting disclosure.

Information need not be highly sensitive in order to be covered by the DPA, but it must not be trivial. The information must not be readily available by other means; this means that it is not covered if it is already in the public domain, or if it is easily obtained. However, it is not necessary that it is completely secret. If the information is very clearly in the public interest, this may override the duty of confidence. The information may relate to an individual in a business capacity (and not just to their private life).

Under the DPA, requesters' identity should be verified in order to avoid making disclosures of information that would breach the Act.

ENVIRONMENTAL INFORMATION REGULATION 1992: 1998 (EIR)

<p>These Regulations establish an access regime that allows people to request environmental information from public authorities and those bodies carrying out a public function Confidentiality clauses do not generally prevent disclosure or sharing of data and there are no other restrictions on data sharing imposed by the EIR.</p>
--

Public access to environmental information is seen as a positive move which will improve environmental protection by increasing public participation in decision-making (UK government sustainable development website: http://www.sustainable-development.gov.uk/what_is_sd/transparency.htm). Environmental information is treated as a specific case (i.e. it is not assumed to be covered by the FOIA) because it has been treated as such in European legislation. For example, requests for environmental information need not be in writing; a wider range of organisations are covered by the EIR, including some private organisations; and the exceptions themselves differ in some respects from the exemptions under the FOIA.

The public has a statutory right of access to environmental information under the Environmental Information Regulations 1992 (SI 3240), for which Defra is responsible. This right stems from a European Community Directive (EC Directive 90/313/EEC on the freedom of access to information on the environment). On 28 January 2003, the 1990 Directive was replaced by a new Directive (EC Directive 2003/4/EC) which takes account of advances in technology, reflects international developments in access rights and also learns from the experience of the earlier regime. New UK Environmental Information Regulations should come into force on 1 January 2005, and the Regulations, consultation document on the Code of Practice, and draft Guidance to the Regulations can be found at: www.defra.gov.uk/corporate/consult/envinfo/index.htm.

These Regulations establish an access regime that allows people to request environmental information from public authorities and those bodies carrying out a public function. Because circumstances vary and change, the Government does not

Annex B. Review of legislation

give a definitive list of organisations subject to the requirements of the Regulations. So organisations will need to take a view themselves as to whether they fall into any of the above categories and it will be for the Courts to decide. In conclusion, any environmental information collected by public bodies (or organisations on behalf of public bodies), is subject to these regulations.

Environmental information is anything that relates to:

- Information on the state the environment and factors affecting the environment, for example, instances of flooding, habitat loss, species extinction, greenhouse gases, radioactive waste, noise, building developments etc.
- Information on measures such as policies, legislation (including reports on the implementation of environmental legislation), environmental agreements etc and also economic analysis/cost benefit of such measures.
- Information on the state of human health and safety, the food chain, cultural/built structures and the conditions of human life, where they are affected by environmental factors such as acid rain, air pollution etc.

The request may be verbal or in writing, and must be responded to as soon as possible, and at least within 20 working days, unless, exceptionally, an extension is needed. The requester may be anywhere in the world, and does not need to say why the information is needed. Requests may only be refused when it is in the public interest to do so, or the information falls within an exemption category. Refusals must be given in writing and the reasons for the refusal must be specified. The Regulations allow the requestor to be charged a reasonable and consistent fee for provision of the information.

The presumption is that environmental information should be released unless there are compelling and substantive reasons to withhold it. Bodies may refuse a request for information that is manifestly unreasonable or is formulated in too general a manner. Further specific grounds for refusing access include environmental information related to: (a) international relations, national defence, public security, (b) legal proceedings, (c) confidential deliberations and internal communications, (d) unfinished documents and (e) commercial confidentiality. Access must be refused if the information is: (a) subject to other statutory restrictions, (b) personal information, (c) volunteered information or (d) potentially damaging to the environment. Certain exceptions including those for commercial confidentiality, and voluntarily supplied data, are not available when the information requested is about emissions into the environment.

Despite the commercial confidentiality exception mentioned above, public bodies are encouraged in the guidance note to the regulations, not to accept confidentiality clauses when entering into contracts with non-public authority contractors. Any non-disclosure provisions could potentially be overridden by the Authority's obligations under the EIR. Any acceptance of confidentiality provisions must be for good reasons and capable of being justified to the Commissioner.

Under this regulation, bodies appear to be under obligation to make clear the level of accuracy of the environmental data they hold. For this reason, Defra suggest that

Annex B. Review of legislation

bodies would be well advised to protect themselves by issuing a disclaimer where appropriate about the accuracy of information that they release to the public and its source.

Bodies are also under obligation to define the practical arrangements under which information is effectively made available. Defra also suggests that: *each body should consider reviewing and stating from time to time the principal areas in which it holds environmental information within the meaning of the Regulations; special mention could be made of any statutory public registers maintained by the body, giving the subject matter covered and the location of each register.* The Regulations do not require the comprehensive publication of environmental information.

In the new EIR, a wider range of organisations is covered (e.g. it includes private bodies or public private partnerships with obvious environmental functions).

RE-USE OF PUBLIC SECTOR INFORMATION REGULATIONS

These regulations concern the re-use of public sector information

These Regulations came into force on 1 July 2005 and establish a framework for making the re-use of public sector information easier and more transparent. They are based on the principles of fairness, transparency, non-discrimination and consistency of application.

The Regulations complement access to information legislation (the Freedom of Information Act, the Environmental Information Regulations and the Data Protection Act) through regulating the re-use of public sector information once it has been made available, either through publishing or in response to a request.

The main elements of the Regulations are:

- there should be a clear statement of copyright ownership on all documents and/or information, together with a statement setting out the arrangements for their re-use;
- there should be greater transparency of licence terms and charges for re-using information.
- an obligation to produce assets lists of information, published and unpublished, which is available for re-use.

PRIVACY AND ELECTRONIC COMMUNICATIONS (EC DIRECTIVE) REGULATIONS 2003

These regulations limit unsolicited direct marketing.

The Privacy and Electronic Communications (EC Directive) Regulations 2003 came into force on 11 December 2003, superseding the Telecommunications (Data Protection and Privacy) Regulations 1999.

The regulations cover:

Telecommunication network and service providers and individuals:

- use of publicly available electronic communications services for direct marketing purposes

Annex B. Review of legislation

- unsolicited direct marketing activity by telephone, by fax, by electronic mail (this means text/video/picture messaging and email) and by automated calling systems,*

Telecommunication network and service providers only:

- processing of electronic communications traffic data
- location data* and billing data
- calling or connected line identification
- directories of subscribers
- the security of telecommunications services and the use of cookie type devices

Note: items marked with * relate to the 2003 regulation only

The Telecommunications Regulations 1999 imposed rules on the use of telecommunications services and gave effect to EU Directive 97/66/EC. One of the main aims of this directive was to ensure the: “protection of fundamental rights and freedoms, and in particular the right to privacy, with respect to the processing of personal data in the telecommunications sector.”

Individuals and corporate subscribers can register their objection to receiving unsolicited direct marketing calls by registering their telephone number with the Telephone Preference Service. Under both the 1999 Regulations and the 2003 Regulations, individuals and organisations have the right to ask the Commissioner to exercise his enforcement functions if they believe they have been affected by a contravention of those Regulations, in respect of e-mails, text messages, faxes, automated calls and telesales.

As these Regulations cover telecommunication network and service providers, and individuals in relation to marketing (for example, the Regulations prohibit the sending of unsolicited commercial email without consent), they do not seem to apply to organisations or individuals using telecommunications to conduct research.

THE COPYRIGHT AND RIGHTS IN DATABASES REGULATIONS 1997

These regulations are about copyright protection of databases. They do not limit data sharing for non-commercial purposes, private study, research, criticism, review or news reporting.
--

The Copyright and Rights in Databases Regulations 1997, SI 1997 No. 3032 came into force on 1st January 1998. They implement European Council Directive 96/9/EC of 11th March 1996, which is a measure designed to harmonise the legal protection of databases throughout the Community. There are two main aspects to the UK Regulations: to change the extent to which the law of copyright will apply to databases, and to introduce a new right, called “ database right”.

Under the Regulations, databases (i.e. printed or computerised collections of information) include both straightforward collections of data such as a list of names and addresses, and more complex collections of materials accessible on-line or on CD-Rom such as an encyclopaedia. A database qualifies for copyright protection under the new Regulations, if it constitutes the author’s own intellectual creation. This means that some originality must have gone into the selection or ordering of the items in the database. Under transitional provisions, any database created before 27th March 1996 (the date of publication of the Directive) which qualified then for copyright

Annex B. Review of legislation

protection, will continue to enjoy copyright protection and will not be affected by the Regulations.

If a database does qualify for copyright protection, “fair dealing” is allowed under a provision. This is use for non-commercial purposes, private study, research, criticism, review or news reporting.

Any copyright which a database may have is separate and independent from any copyright which the contents of the database may have.

The maker of the database (i.e. the person who takes the initiative in obtaining, verifying or presenting the contents and who assumes the risk of investing in the process) is the first owner of the database right in it. The database right will be infringed by anyone who without consent, extracts or re-utilises all or a substantial part of the contents of the database (or repeatedly and systematically extracts or re-utilises insubstantial parts of the contents). The public lending of a copy is not included.

The database right lasts for 15 years from completion, or when the database was made available to the public, or altered substantially. The database right only applies to residents or companies within the EEA. It is therefore advisable to put the name of the maker and date first published on the database, to ensure copyright protection. Database right can be assigned or transferred or licensed.

INTELLECTUAL PROPERTY

Information may be protected by IP rights.
--

Intellectual property allows people to own their creativity and innovation in the same way that they can own physical property. The owner of IP can control and be rewarded for its use, and this encourages further innovation and creativity. In some cases IP gives rise to protection for ideas but in other areas there will have to be more elaboration of an idea before protection can arise. It will often not be possible to protect IP and gain IP rights (or IPRs) unless they have been applied for and granted, but some IP protection such as copyright arises automatically, without any registration, as soon as there is a record in some form of what has been created. The four main types of IP are: patents, trademarks, designs and copyright. It also extends to trade secrets, plant varieties, geographical indications, performers rights and so on.

PUBLIC SERVICE GUARANTEE ON DATA HANDLING

This applies to public bodies and is closely related to the Data Protection Act.
--

The Cabinet recommended that public bodies should support the principles laid down in the Public Service Guarantee on Data Handling, which was implemented in November 2004 and is closely related to the Data Protection Act.

Annex B. Review of legislation

COMPETITION ACT 1998

This Act prevents anti-competitive agreements and behaviour.

<http://www.offt.gov.uk/Business/Legal/Competition/default.htm>

This Act came into force on Mar 2000 and reforms and strengthens UK competition law by preventing anti-competitive agreements and anti-competitive behaviour (abuse of a dominant position in a market).

THE HUMAN RIGHTS ACT 1998

This incorporates into UK law rights and freedoms guaranteed by the European Convention on Human Rights.

<http://www.opsi.gov.uk/acts/acts1998/19980042.htm>

The Act means that all public authorities must pay proper attention to an individual's rights when they are making decisions (departmental for constitutional affairs web site (<http://www.dca.gov.uk/hract/hrafaqs.htm>)).

The Human Rights Act has quite a broad focus and is complemented by the Data Protection Act 1998 and the Freedom of Information Act 2000. By incorporating Convention rights into UK law, the Human Rights Act gives UK citizens a clear statement of their rights and responsibilities. It identifies rights that individuals should be able to enjoy. It also imposes responsibilities on individuals, involving important considerations about balancing their rights with the rights of others and about determining when the State can have good reason to interfere with those rights (Charity commission web site

<http://www.charity-commission.gov.uk/supportingcharities/ogs/g071a001.asp#a1>).