Royal Historical Society

Data Protection and Historians in the UK

July 2020

Katherine Foxhall
RHS Research and Communications Officer

Royal Historical Society

Data Protection and Historians in the UK

July 2020

Katherine Foxhall

RHS Research and Communications Officer
Email address for contact: rescommsofficer@royalhistsoc.org

University College London
Gower Street
London
WC1E 6BT

Contents

Contents	Page 2
Summary	Page 3
1. Introduction: What is Data Protection Law and Why Does it Matter to Historians?	Page 4
2. Geographical Scope of the GDPR	Page 7
3. Personal Data, Processing and Data Controllers: Terminology	Page 8
4. Anonymity	Page 9
5. Exemptions for Historical Research	Page 10
6. Principles for the Processing of Personal Data	Page 12
7. Lawful Bases for Processing Data	Page 13
8. Special Categories of Personal Data	Page 15
9. "Special Purposes" Exemptions	Page 16
10. Working with Archives and Freedom of Information	Page 17
11. Securing and Protecting Data	Page 18
12. Using Personal Data in Teaching	Page 19
13. Data Protection for Historians Checklist	Page 20
14. Other Sources of Information	Page 22
Acknowledgments	Page 22

Disclaimer

The Royal Historical Society has made every effort to ensure the accuracy of the information included here. We do not accept any liability for any consequences resulting from error or omission. These guidelines represent our interpretation of current data protection regulations in relation to historical research; they are designed for general guidance purposes, and do not constitute formal legal advice.

Summary

These guidelines from the Royal Historical Society (RHS) are intended to help historians understand the UK Data Protection Act 2018 (UKDPA). This legislation enacted the EU General Data Protection Regulation (GDPR), which governs how individuals, companies and organisations operating in the EU can process personal data relating to individuals.

This document helps outline historians' responsibilities under data protection legislation, and the exemptions and allowances that attach to historical research.

A checklist (Section 13) is included to help historians demonstrate that they have fulfilled data protection requirements related to historical research.

We welcome feedback, corrections or comments on this document, and will update this Guidance as necessary.

Who is this document for?

- Academic historians, independent historical researchers and genealogical researchers who access, store, or work with historical documents that might identify living individuals;
- Undergraduate and postgraduate students using primary historical material;
- Tutors responsible for students undertaking historical projects with original research (e.g. final year dissertations);
- Tutors using historical documents in teaching that identify, or could identify, living individuals;
- Employers and committees (e.g. with responsibility for funding and ethics approval) wishing to understand exemptions within data protection regulations relating to historical research.

How should this document be used?

We hope that this document will provide a useful resource when:

- planning historical research that may involve material subject to data protection laws;
- preparing requests to access and use archival material about living individuals;
- fulfilling institutional ethics policies relevant to historical research;
- supporting early career researchers, PhD students, and taught students working on historical research projects.

These guidelines should be used with reference to the text of the UKDPA and the ICO Guide to GDPR. We have also provided suggestions for sources of further information at the end. Where relevant, please consult your organisation's Data Officer, and if necessary take specialist legal advice in relation to your specific circumstances.

1. Introduction: What is data protection law and why does it matter to historians?

The EU General Data Protection Regulation (GDPR) came into effect on 25 May 2018.[1] It governs how individuals, companies and organisations operating in the EU can process personal data relating to individuals ("data subjects"), and the rights of those individuals in relation to the data held about them. These reformed data protection laws replaced previous legislation dating from 1995. In response to the technological transformation of data in a digital economy, they were designed to protect online privacy rights.[2]

In the United Kingdom, the GDPR was enacted through the Data Protection Act 2018.[3] Together, the GDPR and UKPDA make up UK Data protection law and will almost certainly continue to do so following the UK's departure from the EU. The UKDPA takes precedence over the GDPR and it is the Data Protection Act that historians in the UK must comply with.

The GDPR requires member states to appoint an independent Data Protection Authority (DPA) to uphold information rights, including the power to implement fines. In the UK, this DPA is the Information Commissioner's Office. As such, the comprehensive ICO Guide to the GDPR is referenced extensively in this document.[4]

Why do historians need to understand Data Protection law?

While most of us encounter the requirements of the GDPR frequently through interactions with websites, companies and other organisations asking for consent to use our data, data protection laws apply to any business, individual, charity, museum, library, research group or project that collects information about a living individual. This includes many historical researchers whether they are working for employment, study, or on a freelance, voluntary or personal basis.

Data protection requirements are clearly relevant to historians working with oral histories, many twentieth-century sources and contemporary material.

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). The GDPR updates and replaces the Data Protection Directive 95/46/EC (1995). The UK DPA replaces and updates the UK Data Protection Act (1998). https://www.gov.uk/government/collections/data-protection-act-2018.

[2] The History of the General Data Protection Regulation https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en

[3] Data Protection Act 2018: http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted.

[4] ICO Guide to the General Data Protection Regulation, version accessed online 4 October 2019. (hereafter ICO Guide): https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/.

While the GDPR does not apply to deceased individuals, it may also be relevant to historical researchers who are using information about a deceased person which could potentially identify, or make identifiable, a living individual in a way that might cause "substantial damage and distress".[5] Examples might include information taken from asylum or medical records, criminal trials, or politically sensitive records relating to topics such as Northern Ireland, civil rights movements, political insurgencies, anti-colonial movements or historic abuse.

Data protection laws will also apply if you collect any forms of documentation containing personal data (e.g. names and/or contact details of participants) while carrying out impact or public engagement activities.

The good news is that data protection legislation based on the GDPR takes a positive approach to research, in particular by enabling the collection and use of data "for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes." The allowances for historical research are examined more fully in Sections 5-8 below.[6]

The GDPR also allows exemptions for journalism, art, literature and academic purposes, which together are known as the "special purposes". These are discussed in Section 9 below.

The GDPR and UK Data Protection Act provide substantial exemptions for research.

The new legislation does not represent a seismic shift in how data can be used in research. It, like previous legislation, is based on principles of fairness, transparency, accuracy, purpose-limitation and security.

The new legislation does represent an opportunity for historians to review their methods and ensure that their use of personal data is fair, lawful, transparent, and does not cause substantial harm, damage or distress to living individuals.

It is likely that the framework of exemptions for historical research that this document covers will be sufficient to enable the majority of data processing that historians need to undertake. As the European Data Protection Supervisor has observed: "respect for personal data is wholly compatible with responsible research".[7]

The Place of historical research within data protection law

Research that advances society's collective knowledge and wellbeing enjoys a privileged position within the GDPR. As the new European privacy regulations were being developed prior to their

[5] The Oral History Society provides a range of clear, useful and up-to-date resources about GDPR: https://www.ohs.org.uk/advice/data-protection/.
[6] See Commentary on Provisions of Act, Section 174: http://www.legislation.gov.uk/ukpga/2018/12/notes/division/6/index.htm.
[7] EDPS "A Preliminary Opinion on data protection and scientific research" (6 January 2020): https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf.

introduction in 2018, many organisations urged the European Parliament and European Commission to protect research.[8] The International Holocaust Remembrance Alliance, an inter-governmental organisation of 31 member countries, argued it was crucial that "the right to be forgotten did not conflict with the responsibility to remember", and emphasised the need for researchers to be able to access Holocaust-related material.[9]

Taking on board such concerns - and substantially continuing the spirit of previous legislation - the GDPR obliges public authorities and private or public bodies to acquire and provide access to records that have "enduring value for general public interest" and that could provide information related to totalitarian state regimes, genocide, crimes against humanity such as the Holocaust, or war crimes.[10]

As the GDPR was being developed and implemented, organisations including the British Academy, ESRC, Royal Geographical Society and British Sociological Association worked hard to ensure that academic expression was shielded on an equal basis to journalism, in order to protect their 'similarly public-focused nature [and] their critical social value', and to prevent universities from interpreting the new regulations in a highly restrictive way through processes such as ethical review.[11]

If a historian's practices complied with previous data protection legislation, they likely still will. While the GDPR does give stronger rights for data subjects, the exemptions attached to academic and historical research are significant.

The key considerations for researchers in using personal data are ethical and practical:

- use of personal data must avoid any likelihood of "substantial damage or substantial distress".
- personal data must be protected against unauthorised or unlawful use and against accidental loss, destruction or damage.
- researchers who make use of allowances and exemptions must document and be able to explain the decisions that have been taken and how they comply with data protection laws.

[8] https://wellcome.ac.uk/sites/default/files/ensuring-healthy-future-for-scientific-research-data-protection-regulation-joint-statement-dec15.pdf
[9] https://www.holocaustremembrance.com/pt-pt/node/699?usergroup=7
[10] Recital 158 EU GDPR: http://www.privacy-regulation.eu/en/recital-158-GDPR.htm.
[11] Joint statement on the implementation of GDPR in UK universities (19 April 2018): https://www.rgs.org/geography/news/joint-statement-on-the-implementation-of-gdpr-in-u/; See also ESRC and British Academy Statement on GDPR (June 2017) https://www.thebritishacademy.ac.uk/documents/103/2017.06_-_BritAc__ESRC_GDPR_Submission_summary_3.pdf.

2. Geographical Scope of the GDPR

This guidance note is written with reference to the UK Data Protection Act 2018, and most references are made to ICO guidelines and the UKDPA (2018). However, because the GDPR is a mandatory framework for the development of legislation by individual member states, much of the information will also be applicable to historians in EU countries, and researchers working with archives in the EU.

EU data protection rules apply in the European Economic Area (EEA), including all EU countries, Iceland, Liechtenstein and Norway. The GDPR applies if you:

- are in the EU and collect or process personal data about a living individual anywhere in the world;
- are outside the EU and collect data on EU citizens;
- plan to share personal data between countries both within and beyond the geographical area covered by the GDPR.

The GDPR contains a number of "derogations", which allow member states flexibility over how certain provisions, particularly relating to data subjects' rights, apply. The UK Data Protection Act adopted these derogations in full (similarly in the Republic of Ireland), but if your research involves research in EU countries, international collaborators or data transfers, you must make sure that you comply with the individual laws of individual member states. Countries with privacy laws based on the GDPR will have similar requirements, but details should be confirmed.[12]

Historians in the UK must ensure that they comply with the UKDPA rather than GDPR wherever they differ.

Historians conducting research in European archives should ensure that their activities are in compliance with the laws of individual member states.

Data Protection and the UK Withdrawal from the EU

The EU has recognised a number of "third" countries as having "adequate" data protection laws, allowing data to be shared between the EU and those countries.[13] Now that the UK has left the EU, it becomes a "third" country, and the UK and EU will need to use the transition period up to 31 December 2020 to come to an agreement about whether the UK has "adequate" data protection laws to allow data sharing between it and EU countries.[14]

[12] A number of resources give comparative information about the adoption of GDPR derogations by member states. See e.g. the GDPR Resource Center Derogations Tracker: https://gdpr.lw.com/Home/Derogations

[13] ICO Guide: International transfers: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/ . On adequacy decisions for third countries: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

[14] GOV.UK: Using personal data in your business or other organisation during and after the transition period https://www.gov.uk/guidance/using-personal-data-after-brexit

3. Personal Data, Processing and Data Controllers: Terminology

Personal data

Personal data is any information that, either on its own, or in combination with other data, allows a *living* individual to be identified either directly or indirectly. Personal data includes names, ID numbers, contact details or location data, appearance, employment details, relationships, personal interests, political or other opinions, or "factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual."[15]

Special categories of data

Special categories of data (previously termed "sensitive data") include race or ethnic origin, religion, politics, trade union membership, health, sexual orientation or activities, criminal convictions, biometric and genetic data.[16] The use of such data is more tightly controlled, but researchers still benefit from exemptions allowing its use (this is discussed more fully in Section 8).

Data Processing

Data processing refers to any operation performed on personal data, whether manually or automatically. This includes the collection, recording, organisation, storage, adaptation or alteration (including anonymisation), retrieval or consultation of information. Processing also refers to how information is used, made available, combined, restricted, shared, published, erased or destroyed.[17]

Data Controllers

Data controllers determine what personal data to process and for what purpose. Anyone who obtains copies of personal data about a living individual, or material that could be used to identify a living individual (e.g. from an archive) becomes a data controller with respect to their use of that information and must observe data protection rules for "processing" that data. Research assistants employed to process data as part of a project do so on behalf of the data controller.

Universities, museums, libraries and archives are also data controllers and must protect their own interests under the GDPR. Many universities are now using ethics procedures to ensure that they document GDPR compliance, and researchers should check their own institutional requirements for using personal data within research and teaching. Organisations are required to appoint a Data Protection Officer, who will be able to provide assistance.[18]

---

[15] Terms relating to the processing of personal data: http://www.legislation.gov.uk/ukpga/2018/12/section/3.

[16] ICO Guide: Personal Data: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/what-is-personal-data/. ICO Guide: Special Category Data: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/

[17] What Constitutes Data Processing? https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-constitutes-data-processing_en/.

[18] ICO Guide, Data Protection Officers: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-officers/.

The term **"Joint controller"** may be relevant when there are two or more controllers (e.g. PIs on a project) who jointly determine the purposes and means of processing personal data. However, people who process the *same* data for *different* purposes, are not considered joint controllers.

Even if your research itself does not fall within the scope of data protection laws, public engagement or impact activities may do if any associated documentation contains personal data (e.g. names and/or contact details of event participants).

Data controllers must keep records in order to be able to demonstrate that they have taken responsibility for processing activities and have put in place measures and records to demonstrate compliance. The checklist at the end of this document (Section 13) is designed to help historians do this.

Data Processors

According to the ICO, "If you don't have any purpose of your own for processing the data and you only act on a client's instructions, you are likely to be a processor – even if you make some technical decisions about how you process the data". In academic contexts, a data processor might include third-party contractors e.g. a website developer or a genealogist employed to carry out a subset of research.[19]

4. Anonymity

Data protection laws do not apply to data that is "truly anonymous". The ICO Code of Practice defines "anonymised data" as "data that does not itself identify any individual and that is unlikely to allow any individual to be identified through its combination with other data."[20] Historians relying on anonymity must take particular care to ensure that there are no "reasonably available means" by which individuals could be re-identified. If these means do exist, data will be considered to have only been "pseudonymised" and will still fall within the scope of data protection laws.

It should be noted that the process of anonymising personal data in the first place is considered to be data processing, and thus is subject to data protection regulations. [21]

[19] The ICO provides useful information about the distinctions between data controllers and data processors, as well as checklists for determining which category you fall into: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/controllers-and-processors/.

[20] ICO, *Anonymisation: managing data protection risk code of practice* (November 2012): https://ico.org.uk/media/1061/anonymisation-code.pdf.

[21] ICO Guide: Anonymous Data: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/what-is-personal-data/what-is-personal-data/

5. Exemptions for historical research

The GDPR provides for a privileged role for research, without making a distinction between research undertaken for scientific, arts and humanities, or statistical reasons. Research should be carried out with the aim of growing society's collective knowledge and wellbeing, rather than simply serving one's own, or private interests.

The European Data Protection Supervisor (the European Union's independent data protection authority) emphasises the need to uphold public trust in research, and that "respect for personal data is wholly compatible with responsible research". The EDPS makes clear that any exemptions from specific requirements (as discussed below) are not a means to justify circumventing data protection safeguards, including:

- processing of personal data must be necessary and proportionate, and not take irresponsible risks.
- researchers must understand, record and be able to explain how and why exemptions are being applied, and how data will be protected both before and after publication.[22]

Data Processing for "scientific or historical research purposes" or "statistical purposes"

Some exemptions and allowances from data protection regulations can apply when data processing is undertaken for "scientific or historical research purposes" or "statistical purposes".[23]

Specifically, where data processing for the purposes of research would be made impossible or seriously impaired by having to comply, research can be exempted from the GDPR's provisions on data subjects' rights related to:

- the right of access;
- the right to rectification;
- the right to restrict processing; and
- the right to object.[24]

[22] EDPS "Preliminary Opinion" (6 January 2020): https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf.
[23] As allowed for within Article 89 of the GDPR . UK DPA (2018) Schedule 2 Part 6 Article 27: http://www.legislation.gov.uk/ukpga/2018/12/schedule/2/part/6/enacted.
[24] Exemptions: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/exemptions/.

In all cases, data controllers must still implement appropriate technical and organisational measures to ensure:

- security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage;
- the safeguarding and protection of the rights of data subjects;
- that personal data is only processed when necessary;
- that decisions about an individual are not based solely on automated processing, including profiling;
- that personal data are not made public by accident;
- appropriate levels of security, including e.g. pseudonymisation and encryption of personal data;
- that any breaches of personal data are notified to the ICO within 72 hours.[1]

Methodological and Ethical Standards in History

The exemptions allowed for research assume that widely-accepted and long-standing sector-related methodological and ethical standards exist which guide research, *in addition to* complying with data protection regulations. These standards are understood as one of the safeguards of the rights of data subjects.

While ethical and professional standards of conduct and practice do not govern historical research in the same way as they do e.g. journalism and clinical trials, there are clear methodological, ethical and professional standards that historians can show that they are taking into account. These include:

- The Royal Historical Society Statement on Ethics available at: https://royalhistsoc.org/rhs-statement-ethics/.
- The American Historical Association Statement on Standards of Professional Conduct (updated 2019): https://www.historians.org/jobs-and-professional-development/statements-standards-and-guidelines-of-the-discipline.[25]
- European Commission, *Ethics in Social Science and Humanities*: https://ec.europa.eu/research/participants/data/ref/h2020/other/hi/h2020_ethics-soc-science-humanities_en.pdf.

[25] The Network of Concerned Historians provides links to various national, international and disciplinary codes http://www.concernedhistorians.org/content/ethichist.html. In addition, a number of individual historians have published useful methodological considerations of ethics in the use of personal data in historical research for use by both professional and non-professional historians. See e.g. Laura Sangha, "The Living, the Dead and the Very Very Dead: Ethics for Historians", https://storyingthepast.wordpress.com/2018/05/22/the-living-the-dead-and-the-very-very-dead-ethics-for-historians-by-laura-sangha/; Antoon De Baets, "A Code of Ethics for Historians (proposal)", in Antoon De Baets, *Responsible History* (2009), 188-196: http://www.concernedhistorians.org/content_files/file/et/148.pdf. Barry Godfrey, Tim Hitchcock, and Robert Shoemaker, "The Ethics of Digital Data on Convict Lives", https://www.digitalpanopticon.org/The_Ethics_of_Digital_Data_on_Convict_Lives.

6. Principles for the Processing of Personal Data

Six principles for the processing of personal data are at the heart of the GDPR and UKDPA. If your use of personal data is for "scientific or historical research purposes" or "statistical purposes", you must comply with these, although some allowances apply.

The six principles are that personal data must be:

a) processed **lawfully, fairly and in a transparent manner**;

b) collected for **specified, explicit and legitimate** purposes and not further processed in a manner that is incompatible with those purposes; further processing is allowed for historical research purposes because it is not considered "incompatible with the initial purposes";

c) **adequate, relevant and limited** to what is necessary in relation to the purposes for which they are processed;

d) **accurate and, where necessary, kept up to date**; In the case of archiving or historical research, data does not need to be kept up to date in the usual sense intended for personal data; as the TNA guide comments, "archives are concerned with historical integrity rather than current accuracy".[26]

e) kept in a form which permits identification of data subjects for **no longer than is necessary** for the purposes for which the personal data are processed. The ICO states that data can be kept "indefinitely" when used solely for historical research purposes, as long as safeguards are in place to protect individuals;[27]

f) processed in a manner that ensures appropriate **security** of the personal data. This includes protection against unauthorised or unlawful processing; accidental loss, destruction or damage; and using appropriate technical or organisational measures to protect data (including pseudonymisation if appropriate).

[26] TNA Guide to Archiving Personal Data, paragraph 40 (hereafter TNA Guide): http://www.nationalarchives.gov.uk/information-management/legislation/data-protection/.
[27] ICO Guide: Principle (e): Storage limitation: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/storage-limitation/?q=indefinite.

7. Lawful Bases for Processing Data

Data protection law requires that anyone processing personal data identifies a lawful basis. This includes if your use of personal data is for "scientific or historical research purposes" or "statistical purposes".

It is important to note that once a basis has been identified, it is not normally possible to change this at a later date. This is particularly significant in relation to consent.

For most historical research three lawful bases (highlighted in **bold** with *) are likely to be appropriate. These are discussed in more depth below.

Lawful bases for data processing:

1) ***the data subject has given consent;**
2) it is necessary to perform a contract;
3) to comply with a legal obligation;
4) to protect the vital interests of the data subject or another person;
5) ***in the public interest or in the exercise of official authority;**
6) ***for the purposes of legitimate interests,** except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject.

Lawful Basis 1) Consent

The GDPR states that consent has to be active, clear, unambiguous, and specific. If you choose consent as your legal basis for processing data, and then consent is withdrawn, you cannot usually choose another legal basis, as noted above.

For this reason, and in line with other organisations, the RHS considers that consent is not usually an appropriate legal basis for historical research.

- **The British Library / Oral History Society** give weight to the importance of 'informed consent' as an *ethical* framework for research practice. They advise that individual researchers should use 'legitimate interests' (see below) as their *legal* basis under the GDPR, and then claim the relevant exemptions for 'scientific and historical research purposes'.[28]
- **UKRI** advise that while seeking consent from people to participate in a project is ethical and may be necessary for other legal reasons (e.g. for medical trials), 'consent', as defined by the GDPR is not likely to be a lawful basis for processing personal data for research purposes".[29]

[28] The Oral History Society provide a useful worked example: https://www.ohs.org.uk/wordpress/wp-content/uploads/Justifying-Oral-History-Sound-Recordings-under-GDPR.pdf. See general OHS advice here: https://www.ohs.org.uk/advice/data-protection/

[29] https://www.ukri.org/files/about/policy/ukri-gdpr-faqs-pdf/; See the TNA Guide, paras 26-28 for specific legal mandates relevant in the UK for archiving in the public interest.

It will be necessary to gain informed consent for any data collected as part of impact or public engagement activities.

While gaining the consent of participants may be morally and ethically necessary (and is considered an appropriate safeguard of data subjects' rights), researchers should not usually rely on consent as the legal basis for processing personal data in order to undertake historical research. Instead, historians should usually consider "public interest" or "legitimate interests" as their legal basis for processing data.

Gaining informed consent *will* be necessary for the use of personal data related to impact, public engagement or similar activities.

Lawful Basis 5) Task in the public interest

Academic researchers employed by UK Higher education institutions, and/or whose work is funded directly by one of the UKRI research councils or an organisation such as the Wellcome Trust, are likely to be able to choose "public task" as a suitable legal basis. This is because provisions for research are explicitly made within individual University Charters, and through legislation such as the Education Reform Act 1988.[30]

UKRI advises its researchers that "public task" is the most likely basis for research in UKRI Institutes and in universities (as public authorities) and that "Using this lawful basis helps to assure research participants that the organisation is credible and using their personal data for public good".[31]

If a "public interest" basis is justified, a researcher must be able to show that the processing of processing personal data is necessary, and be able to "demonstrate there is no other reasonable and less intrusive means to achieve your purpose".[32]

Lawful Basis 6) Legitimate Interest

If a "public interest" legal basis (above) is not available or appropriate (e.g. because you are not employed by a university or similar institution), "legitimate interest" is likely to be the appropriate legal basis for data processing in the case of historical research. What counts as a "legitimate interest" is not clearly defined in GDPR. The ICO acknowledges the flexibility of this legal basis and

[30] Education Reform Act (1988), part 2. http://www.legislation.gov.uk/ukpga/1988/40/part/II, paragraph 124.
[31] UKRI GDPR Guidance for Researchers: https://www.ukri.org/news/general-data-protection-regulation-guidance-for-researchers/
[32] ICO Guide: Public Task: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/public-task/.

notes that "legitimate interests can be your own interests or the interests of third parties. They can include commercial interests, individual interests or broader societal benefits."[33]

For these reasons, the RHS believes that it is appropriate for independent, family and student researchers to identify legitimate interests as their legal basis for data processing.

In such cases, the purposes of the data processing must be specified, explicit, necessary, and respect the rights of the data subject. The ICO clarifies that the term *necessary* "does not mean that processing has to be absolutely essential. However, it must be more than just useful, and more than just standard practice. It must be a targeted and proportionate way of achieving a specific purpose."[34]

8. Special Categories of Personal Data

Data Protection Law generally prohibits the processing of certain "special" categories of personal data, (previously known as "sensitive data").[35] This includes information about:

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- genetic or biometric data for the purpose of uniquely identifying a natural person;
- health, sex life or sexual orientation.

Processing of special categories of personal data is permitted if a lawful basis is identified (see Section 7 above), *and* an appropriate separate condition for processing special category exists. The UK DPA includes historical research as one of these appropriate conditions.[36]

The processing must "be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject."[37]

[33] ICO Guide: Legitimate Interests: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/. E.g. the British Academy Charter (1902) states its role as "the promotion of the humanities and social sciences": https://www.thebritishacademy.ac.uk/about/charter-british-academy.
[34] ICO Guide: Lawful Basis for Processing : https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/.
[35] ICO Guide: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/.
[36] See UK DPA Schedule 1, Part 1 : http://www.legislation.gov.uk/ukpga/2018/12/schedule/1/enacted; GDPR Article 9: http://www.privacy-regulation.eu/en/article-9-processing-of-special-categories-of-personal-data-GDPR.htm.
[37] ICO Guide: Special Category Data: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/.

9. "Special Purposes" exemptions

Section 5 outlined the exemptions related specifically to "historical research". UK data protection law (in full accordance with the derogations provided for within the GDPR) also allows exemptions from more of the obligations of the GDPR and the DPA if you process personal data for "academic purposes" (one of four "special purposes" that also includes journalism, artistic or literary purposes).

The "special purposes" exemptions seem attractive because they potentially relieve data controllers from obligations relating to the basic principles of data protection such as the need to identify a lawful basis; conditions for Consent; processing of special categories of data; and data subjects' individual rights.

Special purposes exemptions can be used if:

- compliance with the GDPR provisions in question would be *incompatible* with (i.e. more than just *inconvenient*) the journalistic, academic, artistic or literary purposes for which data processing is being undertaken;
- "the processing is being carried out with a view to the publication by a person of journalistic, academic, artistic or literary material" ;
- you reasonably believe that publication is in the public interest (which can take into account a general public interest in freedom of expression)
- regulatory codes and guidelines (such as BBC Editorial Guidelines and Ofcom Broadcasting Code) are followed;
- the data controller can explain "why the exemption is required in each case, and how and by whom this was considered at the time". [38]

However, while these provisions appear to offer greater freedom for academics to process personal data than are allowed by the exemptions for "historical research" (Section 5 above) they should be used with care. Recent analysis suggests that the thresholds relating to necessity and publication are high. In addition, data protection regulations are not independent of legislation such as the Human Rights Act (1998) and Equality Act (2010). Because "academic purposes" were a new addition to the category of "special purposes" in 2018, the legal limits to the interpretation of the exemptions for academics have yet to be tested.[39]

The RHS believes that historians should be able to undertake the vast majority of their work using the exemptions and allowances outlined for "historical research" (Sections 5-8 above). The "special purposes" exemptions should only be used when necessary, and expert advice from institutional Data Protection Officers should be sought where appropriate.

[38] UK DPA (2018) Schedule 2 Part 5 Article 26: https://www.legislation.gov.uk/ukpga/2018/12/schedule/2/part/5.
[39] See Miranda Mourby et. al, "Governance of academic research data under the GDPR—lessons from the UK", *International Data Privacy Law*, 2019, Vol. 9, No. 3. Available at https://academic.oup.com/idpl/article/9/3/192/5536592 ; EDPS "Preliminary Opinion".

10. Working with Archives and Freedom of Information

For archives, whether public or private, the concept of "archiving in the public interest" enjoys broadly the same exemptions from the GDPR as are outlined above for "historical research". This means that there should in theory be little conflict between the interests of archives and historians.[40] However, archives have to consider whether giving access to personal data is compatible with data protection law, and researchers may find that some archives - particularly those with limited staff or resources - may have become more cautious in releasing documents in the light of new data protection legislation.

Requesting archival documents

When requesting access to documents that may fall within GDPR regulations, it is helpful for historical researchers to show understanding of their own responsibilities as users of personal data.

In archives, historical researchers may be asked to:

- provide a clear and precise explanation of the exemptions that they are claiming, or the legal basis on which they plan to process data related to living individuals;
- explain how they will undertake historical research within the specified safeguards;
- sign a declaration / undertaking that they will comply with legislation and not identify living individuals unless in ways provided for by data protection law and its exemptions.
- undertake to comply with any sectoral codes of practice or employer requirements such as gaining approval, where appropriate, from University ethics committees. [41]

Freedom of Information requests for information held by a public authority *do not* provide an alternative route for gaining access to archival documents containing personal data. This is because the Freedom of Information Act contains an exemption for personal data, if releasing that data contravenes the GDPR. One important reason for this is that information released under an FOI request has to be made public.

[40] A List of archives that have been approved as Places of Deposit by the National Archives can be found here: http://www.nationalarchives.gov.uk/archives-sector/legislation/approved-places-of-deposit/places-of-deposit/ under Section 4 (1) of the Public Records Act (1958).

[41] TNA GDPR FAQs: https://www.nationalarchives.gov.uk/archives-sector/legislation/archives-data-protection-law-uk/gdpr-faqs/. While the TNA Guide is aimed at the archival sector, it contains a clear and relevant statement (para. 85) about the responsibilities of *users* of archived personal data, which we have adapted here: http://www.nationalarchives.gov.uk/information-management/legislation/data-protection/.

11. Securing and Protecting Data

Securing and protecting data is important for all researchers, but it is imperative that researchers who hold and use copies of personal data in any format, whether paper-based or digital consider and record how they will store, secure and protect personal data to prevent unauthorised or unlawful misuse, loss, or damage.

A number of useful guidelines are available, and researchers should also consult their own institutional Data Protection Officers in order to comply with local requirements:

- The Research Ethics Guidebook: "Data storage and data security": http://www.ethicsguidebook.ac.uk/Data-storage-and-data-security-308.#
- JISC, "Security of Research Data": https://www.jisc.ac.uk/guides/data-protection-and-research-data/security-of-research-data
- UK Data Service, "Store Your Data": https://www.ukdataservice.ac.uk/manage-data/store.aspx.

12. Using Personal Data in Teaching

Student Data

Universities are responsible both for their staff and students' personal data, and for how their students and staff use the personal data of others. Information relating to students including their names, student numbers, attendance and grades are subject to the UKDPA and must be protected.

Using Personal Data in Teaching

As teaching is one of the main functions of universities, "legitimate interest" can be used as a legal basis for using sources that contain personal data within teaching (see Section 7 above). Teaching materials that have been anonymised will not fall in the scope of data protection requirements.

A key consideration when deciding how to use personal data in history teaching, is whether any use of the data is likely to cause "substantial damage or substantial distress" to a living individual.[42]

Student Research Projects

- Students undertaking original research can also claim the exemptions attached to historical research on the basis of "legitimate interest" (see Section 5).
- In most cases, pre-existing procedures for approving project titles and allocating supervisors to students undertaking research projects should be adequate to accommodate data protection considerations.
- Students using personal data should be made aware that they have responsibilities under data protection law, but also the ways that provisions for historical research are built into the legislation.
- Postgraduate students using data collected from, or related to, living individuals may need to go through formal ethics procedures, particularly if they are considering making their work public at a later date.
- Students will also need to consider how to store and protect any personal data that they use.
- Online history collections will often have clear instructions for legal and ethical use of material, and students should be made aware of the need to follow these.

[42] ICO Guide: Exemptions: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/exemptions/. See also Data Protection Act 2018, Section 19: http://www.legislation.gov.uk/ukpga/2018/12/section/19.

13. Data Protection for Historians Checklist

☐ Q. 1. Does my research, teaching or other activity e.g. public engagement use personal data about living individuals?

☐ Q. 2. Does my research use data about deceased individuals that could potentially cause substantial harm or distress to living individuals?

If yes to either of the above questions:

☐ Q.3 Does my research fall within the GDPR's geographical scope? *(See Section 2)*

☐ Q.4 Is my data anonymous, or can I anonymise the data so that it no longer falls within the provisions of the GDPR? *(See Section 4)*

Data Processing for "Scientific or Historical Research Purposes" or "Statistical Purposes"

☐ Q.5 Is my use of personal data for "scientific or historical research purposes" or "statistical purposes"? *(See Section 5)*

☐ Q.6 Am I following ethical and methodological guidelines in undertaking my research project? *(See Section 5)*

☐ Q.7 Have I complied with the main principles for the processing of personal data, notwithstanding the allowances for research? *(See Section 6)*

☐ Q.8 Have I identified and recorded a legal basis for the use of this personal data? *(See Section 7)*

☐ Q.9 Do I need to gain consent for the use of personal data? *(See Section 7)*

☐ Q.10 Does my personal data include "special category" data, and if so, do the purposes of my work permit me to process that data? *(See Section 8)*

Cont.

Data Processing for "special purposes"

☐ Q.11 Does my use of personal data meet the criteria for the "special purposes" of researching or publishing for journalistic, academic, artistic or literary purposes? *(See Section 9)*

All of the following criteria must be considered in answering this question:

- Is using this exemption absolutely necessary?
- Would complying with the relevant GDPR requirements be *incompatible* with my purpose for processing this data?
- Is my data processing undertaken primarily with a view to publication?
- Is my processing of this personal data in the public interest?
- Can I justify why I believe the exemption is required in each case?
- Have I recorded how and by whom this was considered at the time?
- Does my use of personal data within these criteria still comply with the basic concepts that underpin GDPR (i.e. those of fair, open and reasonable use, and avoiding material and non-material harm)
- Am I aware of how other legislation may be relevant to my use of personal data?
- Have I consulted with an institutional data protection officer?

In *all* cases:

☐ Q.12 Have I documented:

- what personal data I hold;
- where the data came from;
- who it will be shared with;
- what I plan to do with it?
- any exemptions that I consider to be relevant?
- how I will secure and protect the personal data that I am in control of? *(Section 10)*

Archives

☐ Q.13 Does the archive I am using require me to to gain formal approval for my use of personal data e.g. through institutional ethics processes? *(See Section 11)*

Teaching

☐ Q.14 Have I considered if my use of personal data in teaching may be subject to data protection requirements? *(Section 12)*

14. Other Sources of Information

Information Commissioner's Office Guide to the Data Protection Regulation (296 pp)

The National Archives has produced a detailed and comprehensive Guide to Archiving Personal Data in co-operation with the archives sector.

The Oral History Society online guide to GDPR is specifically for researchers undertaking oral history interviews, but is also generally applicable for understanding how GDPR relates to historical research.

The Collections Trust Guidance Document emphasises fairness, and covering aspects of data protection law of particular relevance to museums.

IAPP website "How GDPR changes the rules for research", a useful article on processing for research purposes.

UK Anonymisation Network: https://ukanon.net/ukan-resources/ukan-decision-making-framework/.

EDPS "A Preliminary Opinion on data protection and scientific research" (6 January 2020): https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf.

Acknowledgments

The author is grateful to all those who contributed their ideas, expertise, assistance and feedback on earlier versions of this document including: Laura Carter, Jay Fedorak, Margot Finn, Jonathan Fryer, Valerie Johnson, Jonathan Morris, Robert Perks, Mark Roodhouse, Andrew Smith, Linda Stewart, Mary Vincent, Pippa Willcox, Jane Winters, Members of RHS Council.

Dr Katherine Foxhall
Royal Historical Society
July 2020
rescommsofficer@royalhistsoc.org