

Retaining personal records... through time

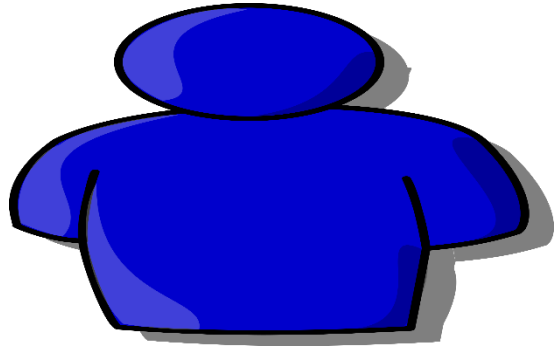
Dr Elizabeth Lomas, UCL

e.lomas@ucl.ac.uk

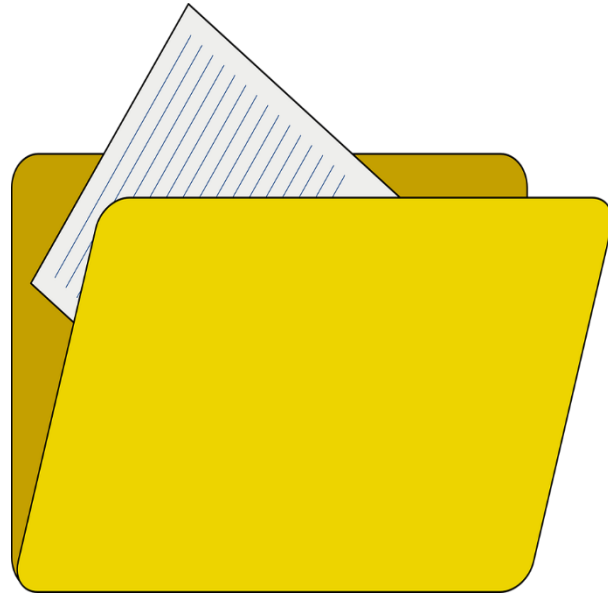


Dictated how we must 'process'
'personal data'

Not a substitute for legal guidance!



**100 Years for
an individual!**



- Freedom of Information
- Confidentiality
- Human Rights Act 1998



Dictate how we must 'process'
'personal data'
Builds on Data Protection Act 1998

- Susan Healy
- LSWG, ARA, Susan Graham

- Suzie Mereweather and Sonja King

- Guide to Archiving Personal Information in the Public Interest
The National Archives – Stuart Abraham, Malcolm Todd and Anna Sexton
National Records of Scotland – Laura Mitchell and John Simmons
Museums, Archives and Libraries, The Welsh Government – Mary Ellis and Sarah Horton
Public Record Office of Northern Ireland – David Huddleston and Jayne Hutchinson
Archives and Records Association (UK and Ireland) – Jon Elliott
National Archives, Ireland - Niamh McDonnell

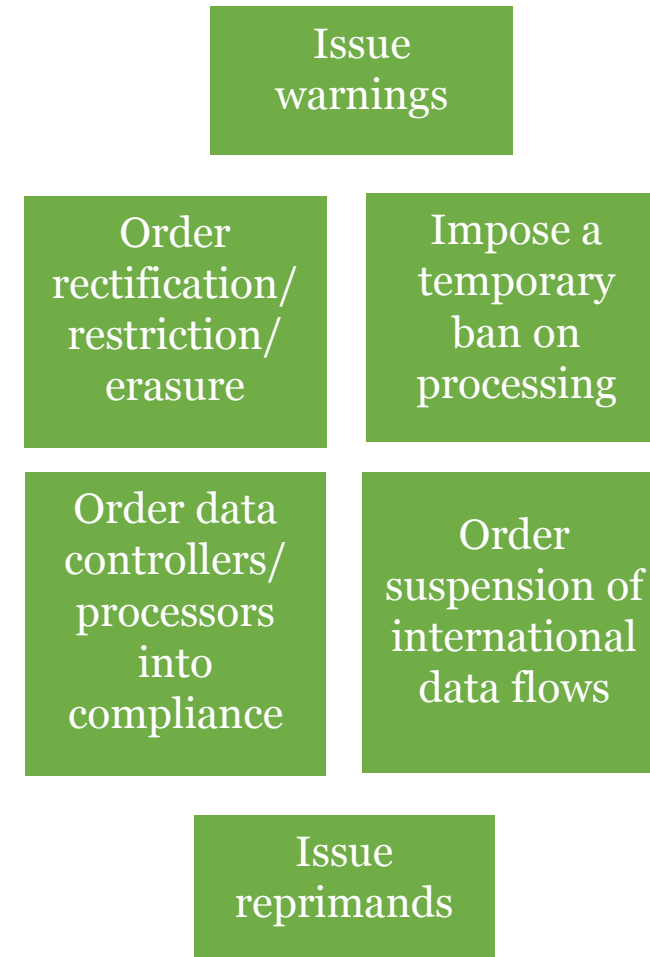
Fines of up to 20 million Euros or 4% turnover (whichever is greater)

Wrongly applying processing conditions (especially consent)	Transferring personal data overseas without appropriate safeguards	Failing to meet a subject access request
		Infringing the rights of an individual

Fines of up to 10 million Euros or 2% turnover (whichever is greater)

Failing to report breaches to the ICO	Failing to ensure all safeguards are in place when using a data processor	Failing to practise privacy by design
---------------------------------------	---	---------------------------------------

ICO can also...



Personal data: Data by which a living individual (data protection subject) can be identified:

- Name
- Address
- Date of birth
- Gender
- Biographical information
- Opinions
- Image, ie photograph
- Some online identifiers – IP address

Sensitive personal data: Data which is of a private nature and could be used in a discriminatory way:

- Ethnicity
- Disability
- Physical or mental health
- Sexuality
- Religious (or similar) belief
- Union membership
- Political opinions
- Can include Image (if the image demonstrates any of the above)
- Biometric data

There are stricter rules for managing sensitive personal data.

“sufficient understanding and maturity”
Gillick v. West Norfolk AHA [1986] AC 112

DPA 2018

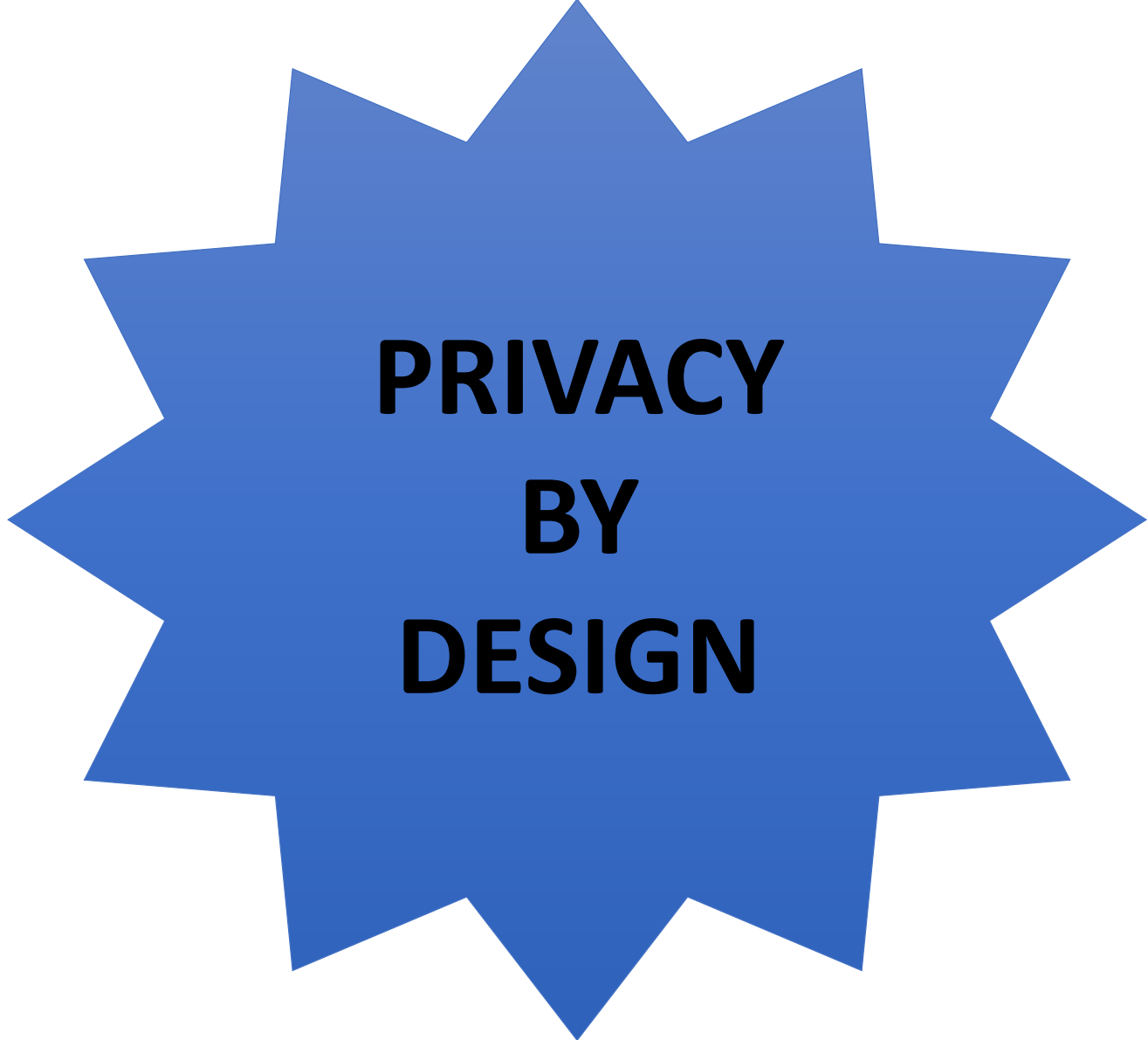
Consent from age 13 years old

ICO “ We allow competent children to exercise their own data protection rights. ”

Design systems

To ensure age is known

Transparent and fair with children in mind

A large, blue, multi-pointed starburst graphic with a jagged, sunburst-like edge, centered on the page. It contains the text "PRIVACY BY DESIGN" in bold, black, uppercase letters.

**PRIVACY
BY
DESIGN**

GDPR Article 5(1)(c)

Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

GDPR Article 25(2)

The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the period of their storage and their accessibility.

GDPR - Article 24(1)

Taking into account the nature, scope, context and purposes of the processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. These measures shall be reviewed and updated where necessary.

GDPR Article 35

The controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.

The assessment shall contain:

- A systematic description of the envisaged processing operations and the purposes of the processing
- An assessment of the necessity and proportionality of the processing operations in relation to the purpose
- An assessment of the risks to the rights and freedoms of the data subject
- The measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation

GDPR - Article 30

Each controller...shall maintain a record of processing activities under its responsibilities. The record shall contain:

- (a) the name and contact details of the controller...;
- (b) the purposes of the processing;
- (c) a description of the categories of data subjects and of the categories of personal data;
- (d) the categories of recipients to whom the personal data have been/will be disclosed;
- (e) where applicable, transfers of personal data to a third country...;
- (f) where possible, the envisaged time limits for erasure of the different categories of data;
- (g) where possible, a general description of the organisational and security measures.

GDPR Article 15

The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed...The controller shall provide a copy of the personal data undergoing processing.

- Fair
- Lawful
- Transparent
- Portability
- Rectification, locking, erasure or destruction
‘Right to be forgotten’

- Damage/substantial damage
- Distress/substantial distress

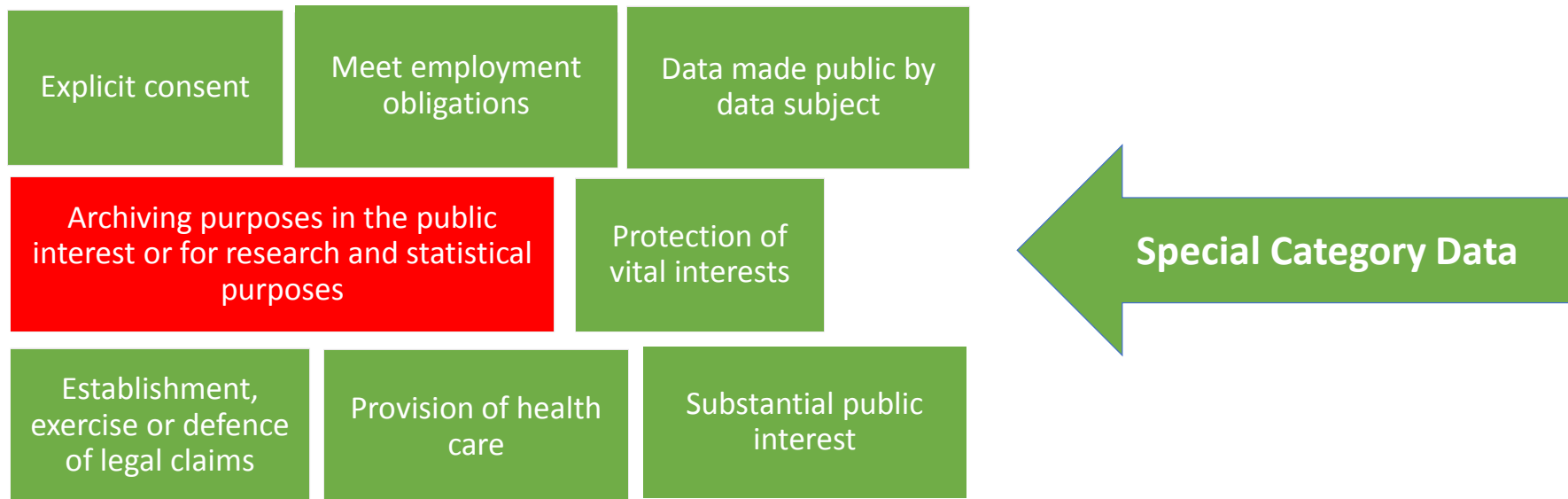
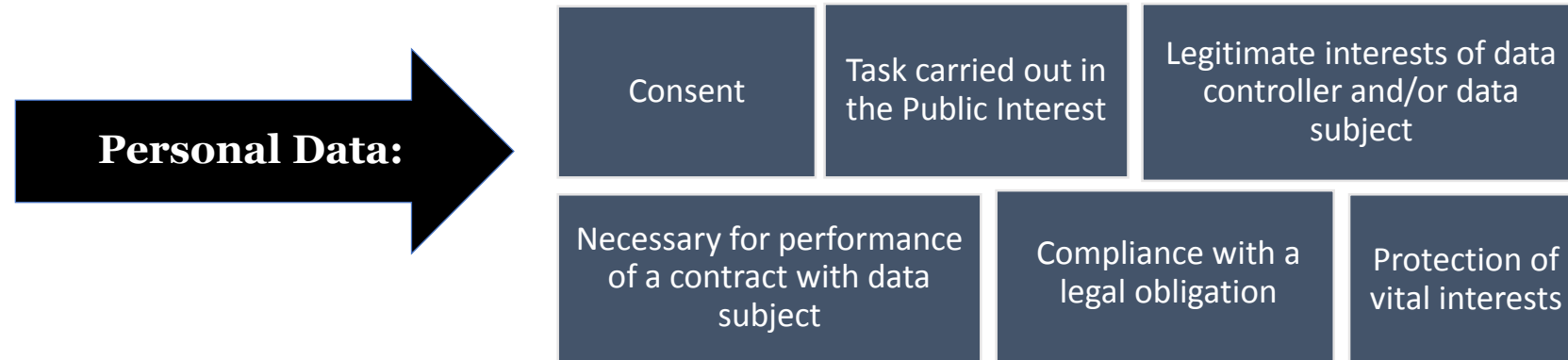
What is meant by “substantial damage or distress”?

The Act does not define this. However, in most cases:

- substantial damage would be financial loss or physical harm; and
- substantial distress would be a level of upset, or emotional or mental pain, that goes beyond annoyance or irritation, strong dislike, or a feeling that the processing is morally abhorrent

Substantial’ often deemed to be ‘enduring’

Legal basis for processing



Key tools: Privacy Notice and Consent Processes

1. processed **lawfully, fairly** and in a **transparent** manner in relation to individuals;
2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing **for archiving purposes in the public interest, scientific or historical research purposes** or **statistical purposes** shall not be considered to be incompatible with the initial purposes;

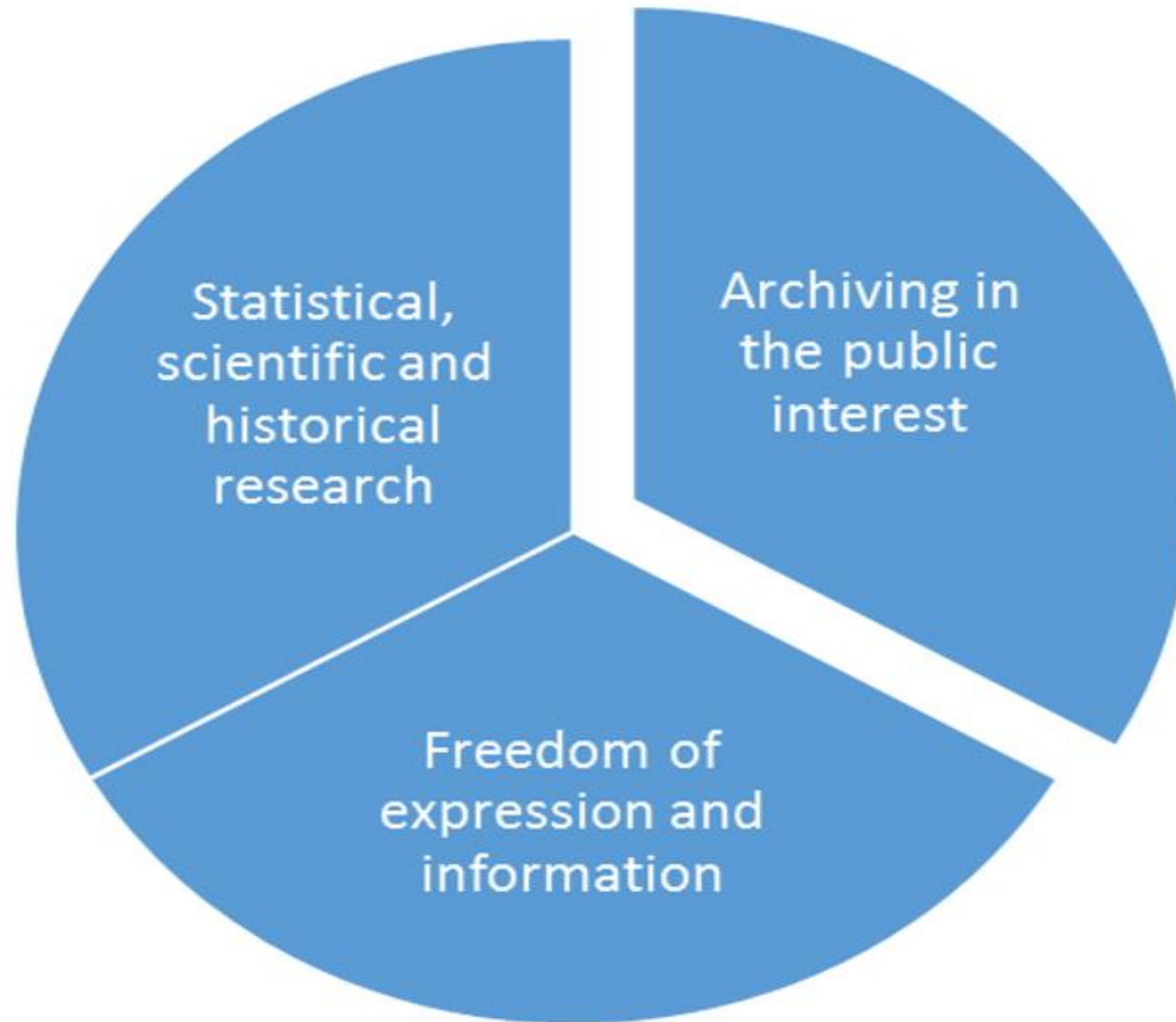
3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
4. accurate and, where necessary, kept up to date;

5. 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; personal data may be stored for longer periods insofar as the personal data will be processed solely for **archiving purposes** in the public interest, scientific or **historical research** purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures;

6. processed in a manner that ensures **appropriate security** of the personal data, including protection against **unauthorised** or **unlawful processing** and against **accidental loss, destruction or damage**, using appropriate technical or organisational measures.

An information security breach is considered to be any loss of, or unauthorized access to, information, normally involving personal or confidential information including intellectual property. Information security breaches include the loss or theft of information or equipment on which information is stored, inappropriate access controls allowing unauthorised use, human error (e.g. information sent to the incorrect recipient), hacking attacks and ‘blagging’ or social engineering, where information is obtained by deception.

- 72 hours reporting deadline
- Investigations do fine if information breached should no longer have been held



See for further information The National Archives (2018) *Guide to archiving personal data*. London: OPSI. Available at: <http://www.nationalarchives.gov.uk/information-management/legislation/data-protection/>. (Accessed 22 September 2018).

Elizabeth Denham, Information Commissioner:

“Archives are special places. They are our collective memory. They help us to understand the past, make sense of the present, and guide us for the future. And in an age of fake news, misinformation and opaque institutions, archives are more important than ever in helping to uphold democracy and hold power to account.”

The National Archives (2018) *Guide to archiving personal data*. London: OPSI., p.4.

WHY?

WHEN?

WHAT?

WHERE?

**PROCESSING FOR ARCHIVING PURPOSES IN THE
PUBLIC INTEREST**

WHO?

HOW?

HOW
MUCH?

PROCESSING FOR ARCHIVING PURPOSES IN THE PUBLIC
INTEREST – R 156, 158

Legislation
or other law
re archives

OR

Government
'policy' (WA
111381)

PLUS

Publicity to
provide R 41
foreseeability

AND

Compliance
with
safeguards

EQUALS

Acceptable
claim of
APIPI

✓ Records of enduring value

X If personal data is being kept solely for a defined business or legal purpose and the intention is to destroy it after that has finished, this is not archiving in the public interest.

- *Article 15(1) to (3) (confirmation of processing, access to data and safeguards for third country transfers);*
- *Article 16 (right to rectification);*
- *Article 18(1) (restriction of processing);*
- *Article 19 (notification obligation regarding rectification or erasure of personal data or restriction of processing);*
- *Article 20(1) (right to data portability);*
- *Article 21(1) (objections to processing)* If personal data is being kept solely for a defined business or legal purpose and the intention is to destroy it after that has finished, this is not archiving in the public interest.

The exemptions are not automatic. Their use is subject to appropriate safeguards for the rights and freedoms of data subjects.

Article 89(1) of the GDPR says that those safeguards must include the implementation of technical and organisational measures.

- *Article 15(1) to (3) (confirmation of processing, access to data and safeguards for third country transfers);*
- *Article 16 (right to rectification);*
- *Article 18(1) (restriction of processing);*
- *Article 19 (notification obligation regarding rectification or erasure of personal data or restriction of processing);*
- *Article 20(1) (right to data portability);*
- *Article 21(1) (objections to processing)* If personal data is being kept solely for a defined business or legal purpose and the intention is to destroy it after that has finished, this is not archiving in the public interest.



MIRRA

Memory – Identity – Rights in Records – Access

Year One Project Report

Achievements, Early Findings and Actions

Professor Elizabeth Shepherd

Dr Andrew Flinn

Dr Elizabeth Lomas

Victoria Hoyle



Arts & Humanities
Research Council



Early Findings – Access to Records

- Provision of access to records is inconsistent.
- Protocols and procedures fail to account for the needs of care leavers.
- Experiencing access to files is a complex affective process that is ‘double-edged’
- There is potential for re-traumatising *but also for* vindication
- Lack of contextual and ‘pre-access’ information.
- Dynamics of power and lack of self-determination experienced in childhood are replicated, symbolised by redaction.
- Redaction is the pressure point for both care leavers and practitioners.
- Practitioners are faced with challenging decisions, often with no specific training.
- Practical issues and lack of resources make change difficult.
- Motivations to access records are complex and multiple.
- Access is not a single moment in time.

Early Findings – Access to Records

Quote from workshop with care leavers:

So you assume because of the way that you are being treated that you are bad, that it is your fault, that you are in the wrong, and I have had to keep saying to myself 'no I am alright me' but there was things written in the file like that I was the rejected one, it was written too many times to be the opinion of one person...So for me it was confirmation that I was rejected by my mum, that it wasn't my fault

Early Findings – Recordkeeping Practices

- Recording is ubiquitous but onerous, focused on managing risk.
- Digital systems have generated new recordkeeping practices.
- Lack of integration between life story work and personal memory curation and the ‘official’ record.
- Absence of the voice of the child, young person and family.
- Records management of child social care records is uneven.
- Multiple and overlapping recording systems, and the shift from analogue to digital, are confusing.
- Information sharing between agencies is a source of anxiety.

Early Findings – Regulation and Legislation

- Legislation on the retention and management of records no longer reflects care practices.
- Data Protection legislation does not adequately provide for people whose personal histories are held by organisations.
- Disparity of rights and provision of services between groups, e.g. enhanced rights of adopted adults.
- Rapidly evolving landscape with the implementation of GDPR and the DPA 2018.

Contact: Dr Elizabeth Lomas, Senior Lecturer in Information Governance e.lomas@ucl.ac.uk

Professor Elizabeth Shepherd, Principal Investigator

Dr Andrew Flinn, Co-Investigator

Victoria Hoyle – Research Associate, UCL

v.hoyle@ucl.ac.uk

Website: <http://blogs.ucl.ac.uk/mirra>

Twitter: @mirraproject

MIRRA
MIRRA



Arts & Humanities
Research Council