Sanctions for Personal Data Misuse: Evidence Paper

The regulatory landscape regarding sanctions for data misuse in the UK is complex. For researchers and institutions this means it can be difficult to decipher exactly what the possible sanctions are, when they can be applied, and who should enforce them. This difficulty can result in two kinds of outcomes: researchers and institutions become risk-averse and withhold access to all research data for fear of breaching data protection laws; or, unaware of their responsibilities and obligations towards protecting the data, they are too lax about data security and management, allowing data to be shared inappropriately or without due safeguards.

Hence EAGDA asked the Secretariat to provide evidence on what sanctions currently exist for misuse of data, encompassing the legal and regulatory context and the bodies or organisations that may exert influence over researchers. "Misuse" in this report is taken to mean the unauthorised or unethical use of data from participants in research or patients. This evidence in this paper was collected through desk research in response to that request and covers two broad domains:

- The legal and regulatory framework relevant to sanctions for the types of data misuse that could arise in scientific research in the UK, including the new EU General Data Protection Regulation.
- The landscape of sanctions for data misuse that could be imposed on researchers by: funders; institutions; repositories; research consortia and journals.

1. UK legislation for personal data misuse

The underlying legal basis for punishing the misuse of personal data is to protect the right to privacy, which is currently enshrined in UK law via the 1995 EU Data Protection Directive[1]. This explicitly linked the notion of privacy with people's fundamental rights and freedoms with respect to the processing of personal data, to enable individuals to control information about themselves. The Human Rights Act (HRA) also safeguards the right to respect for private life, including the right to respect for personal information, under Article 8 of the European Convention on Human Rights.[2] This entails that failures of data protection may contravene a person's human rights.

There is a patchwork of law governing the use of personal data, which can make it difficult to navigate. The legal framework would not apply to data that has been de-identified, although there is a significant grey area for data that is potentially re-identifiable (which depends on the data environment). Much research use of data would fall into this category. For the purposes of this report, we include only legislation that makes explicit reference to punishments for wrongdoing in relation to research uses of data.

[1] The scope of this report is limited to the UK; however as UK and EU law are (currently) intrinsically linked, EU laws are reported where appropriate.

[2] "The protection of personal data, particularly medical data, is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life as guaranteed by Article 8 of the Convention." (MS v Sweden (1997) 28 EHRR 313, para. 41, as quoted http://www.publications.parliament.uk/pa/jt200708/jtselect/jtrights/72/72.pdf p.11) [Accessed 12 July 2016]

Scope of sanctions within UK/EU legislation

Legislation	To what does this legislation apply?	Definition of 'personal data'*	Definition of 'data misuse'*	Sanctions available
Data Protection Act (1998)	All personal data (UK)	- Data directly identifies individual. - Identity can be deduced from data. - Identity can be deduced in combination with other data sets.	If the data controller: - Violates the data protection principles. - The violation is likely to cause substantial harm or distress - The violation was deliberate - Or, the data controller knew a violation that could cause distress would occur.	- Up to £500,000 fine - Order for destruction of relevant data
EU General Data Protection Regulation (2018)	All personal data (EU)	- Data relating to an identifiable person. - Identity can be deduced either directly or in combination with other data sets by the data controller or **by another person**.	- Violations of a large range of articles listed within the GDPR.	- Up to £20,000,000 fine or 4% of global turnover, whichever is higher
Statistics and Services Registration Act (2007)	Statistical information held by the UK Statistics authority (UK)	- Data directly identifies individual. - Identity can be deduced from data. - Identity can be deduced in combination with other data sets.	- Disclosure of personal information by member or employee of the Statistics Board or anyone who has directly received data from the board.	- Fine or custodial sentence of up to two years
Digital Economy Bill (In draft, passing through parliament)	Personal data held by government authorities (UK)	- Data directly identifies individual. - Identity can be deduced from data. - Identity can be deduced in combination with other data sets.	- Same as DPA. - A bar on further disclosure exists if the person responsible for disclosing the data received it from a government department for the purposes of processing	- Same as DPA - In addition: fine or custodial sentence up to two years.

Table 1: Legal basis of sanctions for data misuse (UK/EU)

*See appendices for full legislation text.

Data Protection Act (1998)[3]

The Data Protection Act (DPA) is the current legislation defining sanctions for misuse of personal data in the UK and is enforced by the Information Commissioner's Office (ICO)[4]. It will be supplanted by the EU GDPR, or by any equivalent law the UK government passes post Britain's exit from the European Union. Financial penalties exist for breaches of the DPA and the ICO can order data to be destroyed to prevent further breaches.

Under the DPA, any processing of personal data needs to have a legal basis otherwise it is unlawful. For research in many instances this legal basis will be consent

[3] http://www.legislation.gov.uk/ukpga/1998/29/contents (s.55 and s.60) [Accessed 15 July 2016]
[4] http://ico.gov.uk [Accessed July 2016]

There is an existing legislative instrument for criminal sanctions to be used via amendments to the DPA, but it has not been enacted despite the ICO and other stakeholders calling for this for several years. Section 77 of the Crime and Immigration Act (2008) makes provision for an amendment to the DPA to enforce custodial sentences of up to 2 years for the most serious breaches of s.55 of the DPA.[5]

EU General Data Protection Regulation (EU GDPR)[6]

A new EU wide data protection regulation was agreed in December 2015. It is due to be implemented in May 2018. If the UK wishes to participate in data sharing with rest of the EU, then it must either adopt the EU GDPR or pass legislation that fully aligns with its principles.

Criminal penalties for data misuse are delegated to member states (recital 149).The GDPR does not impose any EU wide criminal sanctions for data misuse. Any criminal sanctions enacted in the UK are likely to be similar to those already in existing statutes (outlined below). The UK Government is currently considering how best to enact the GDPR in light of Brexit and has not yet decided whether this will be via primary or secondary legislation.

NHS Act (2006) – s.251

If consent is not possible or feasible to obtain for uses of health or medical data, applicants who wish to use personal data for a medical purpose may apply for a s.251 approval via the Confidentiality Advisory Group of the Health Research Authority (in England and Wales). Approval via this route enables the common law duty of confidentiality to be set aside for a specific purpose. Data users still have to comply with the provisions of the Data Protection Act, and must abide by standard conditions of approval which include the provision that any staff who have access to the data must have "contractual obligations of confidentiality, enforceable through disciplinary procedures"[7]. Data users must facilitate and support any audit carried out and any breaches of confidentiality must be reported to CAG within 10 working days, along with reporting on remedial actions.

There is no further information available on sanctions for misuse or whether data users would have access to data withdrawn or refused in future under these circumstances.

Statistics and Registration Services Act (2007) (SRSA)[8]

The SRSA governs the confidentiality of personal information held by the UK Statistics Authority and its executive office, The Office for National Statistics. The Statistics Authority is an arm's length body producing official statistics for the UK government, often derived from personal data. The SRSA includes criminal sanctions: custodial sentences of up to two years for the disclosure of personal data that is not subject to a specific list of exceptions (concerning fulfilling statutory obligations, disclosure via consent, and use by an 'approved researcher' (s.39(4)).

The Digital Economy Bill[9]

[5] http://www.legislation.gov.uk/ukpga/2008/4/section/77 [Accessed 15 July 2016]
[6] http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf [Accessed 15 July 2016]
[7] Para 5: http://www.hra.nhs.uk/documents/2015/09/cag-standard-conditions-approval-2.pdf
[8] http://www.legislation.gov.uk/ukpga/2007/18/pdfs/ukpga_20070018_en.pdf (s.39) [Accessed 18 July 2016]

The Digital Economy Bill was introduced to Parliament just before the summer recess of 2016. It is a wide-ranging piece of legislation that seeks to improve data sharing between government departments and the use of administrative data for the purposes of research and statistics. The Bill includes clauses that would introduce criminal sanctions similar to those set out in the SRSA, which would apply to data held by public bodies.

The Bill specifically excludes health and medical data used for research from its remit. It does not currently include sharing of health and medical data for the delivery of public services, but the Government has acknowledged it may seek to include health and social care bodies through secondary legislation in the future. It is unclear whether this will include harmonising sanctions for misuse of data. There is significant objection to clauses in the Bill that appear in principle to set aside the common law duty of confidentiality in relation to health and care data.[10]

Computer Misuse Act (1990)

Reference to this Act is included in this scoping as it creates sanctions for the misuse of computing systems to access data without appropriate authorisation. Its primary focus is on computer hacking and the general sanction for any violation of the Act is a prison term not exceeding twelve months or a fine not exceeding the statutory maximum. The Act may be beyond the scope of interest for the misuse of personal data in a research context because it explicitly concerns unauthorised *access* to a system, i.e., hacking. It would not apply in the scenario likely to arise with research whereby a researcher does have authorised access to a system but uses the data in an unauthorised way[11].

Common Law

Common Law of Confidentiality (CLC)

This is a law set by precedent rather than legislation. It derives from case law judgements and as such does not set down a specific set of criteria for what constitutes a breach of confidentiality. Primarily it is used in healthcare, forming part of the NHS confidentiality policy.

The common law of confidentiality states that any information recorded about a patient may not be disclosed without permission. It can be set aside under Section 251[12] of the NHS Act 2006, subject to approval by the Confidentiality Advisory Group of the Health Research Authority. This exemption was specifically passed to enable use of patient data in research.

Breaches of the CLC are a civil, not a criminal matter. People affected by a data breach can seek redress and claim damages. Orders can also be made to deliver and destroy infringing

[9] http://services.parliament.uk/bills/2016-17/digitaleconomy.html [Accessed 30 March 2017]
[10] See for example https://www.bma.org.uk/news/2017/february/data-sharing-bill-threatens-patient-confidentiality
[11] http://www.brodies.com/blog/the-computer-misuse-act-a-beginners-guide/ [Accessed 21 July 2016]
[12] http://www.hra.nhs.uk/about-the-hra/our-committees/section-251/what-is-section-251/ [Accessed 23 July 2016]

materials and accounts of profits[13]. This contrasts with other legislation that gives courts and commissioners the power to impose fines on guilty parties, without compensating victims.

Current context for policy on sanctions

'Big Data Dilemma'

In the 2015-16 Parliamentary session, the House of Commons Science and Technology Committee held an inquiry on 'The Big Data Dilemma'[14], which sought to identify the challenges and opportunities represented by emerging data technologies for the UK. Sanctions regarding misuse of personal data formed a significant part of the discussion:

- Concerns were raised during the inquiry that issues such as risk of re-identification from existing datasets are not covered by existing UK legislation. Malicious or deliberate attempts to re-identify individuals would not fall under data protection legislation unless the attempts were successful (and thus resulted in the user holding personal information). Several stakeholders, including the Wellcome Trust, argued that unwarranted attempts to re-identify from de-identified data should be punishable.
- The ICO wished to implement custodial sentences, provided for in The Criminal Justice and Immigration Act via amendments to the DPA (see above).
- The Government responded that sanctions put in place by the EU GDPR would be enacted and tested before introducing any further penalties for misuse of data into UK law.
- The Government has indicated it will take up a recommendation of the inquiry to create a 'Council on Data Ethics', based at the Turing Institute, which will explore ethical issues emerging from the development and implementation of big data technologies. This is likely to include discussion of data governance and what appropriate sanctions would look like.

National Data Guardian Review

In June 2016 the National Data Guardian for Health and Social Care, Dame Fiona Caldicott, launched a Review into data security and patient consent/opt-outs for the use of personal information (held within/by the health and social care system) for purposes beyond direct care. The Review recommended *"there should be much tougher sanctions for malicious or intentional data security breaches."* [15] Details on what these sanctions might be were not provided. The Department of Health consultation on the Review's recommendations closed in September 2016 and a response is expected after Easter 2017.

2. Sanctions policies in practice

The Secretariat undertook desk research to identify what sanctions for the misuse of data could be imposed by research funders, institutions, research consortia, data repositories and

[13] http://www.inbrief.co.uk/contract-law/breach-of-confidence/ [Accessed 23 July 2016]
[14] http://www.publications.parliament.uk/pa/cm201516/cmselect/cmsctech/468/468.pdf [Accessed 30 June 2016]
[15] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/535024/data-security-review.PDF (para 1.17) [Accessed 1 July 2016]

journal publishers. This information was compiled by reviewing publicly available policies on research integrity, good research practice, research misconduct, privacy/data security and data access and management terms. At present, relevant funder policies do not go into sufficient detail to enable a more fine-grained analysis of whether and how they are being implemented in practice, or what effect they have on researcher behaviour. The information presented here summarises the key findings with particular focus on existing funder approaches.

2.1 Relationship between legal framework and sanction policies

The majority of policies do not make a connection between researchers' responsibilities, together with the penalties for failing to abide by these, and the law on personal data misuse.[16] If policies make any reference to the legal context it tends to be in vague terms, such as stating that "researchers should comply with UK laws."

There are some exceptions, with organisations that have policies explicitly referring to the regulatory framework and specifying what sanctions are applicable in relation to these:

Administrative Data Network (ADRN)

- As the ADRN facilitates the use of government-held data, it has a comprehensive breaches policy. It specifically states that sanctions put in place by the ADRN do not exclude the possibility of being prosecuted under the DPA or SRSA.

UK Data Service (UKDS)

- The possibility of the Office of National Statistics prosecuting individuals under the SRSA is highlighted in their Secure Lab Breaches policy.[17]

Scottish Informatics Program (SHIP)

- SHIP provides a toolkit on the linkages, at a regulatory level, between research and data access.[18] This toolkit contains regulatory guidance aimed at researchers. This is not seen in other sanctions policies.
- Included within this toolkit is a detailed summary of the DPA.

Administrative policies

Many institutions do include references to regulation (mainly DPA and SRSA) when referring to **non-research personal data**. This tends to be where it concerns the management of personal data about staff or students and is targeted at administrators and managers. These policies regarding the misuse of personal data are often clearly linked to the DPA.

A disconnect exists between how institutions treat administrative personal data misuse and the misuse of personal data in research. The same principles may apply to both types of

[16] For example, the UK Research Integrity Offices (UKRIO) code of practice for good research makes no explicit link between research conduct and regulation, and the DPA is mentioned only in the bibliography.
[17] https://www.ukdataservice.ac.uk/media/176861/UKDA142_SDS_SecurityBreaches_public.pdf [Accessed 27 June 2016]
[18] http://www.scot-ship-toolkit.org.uk/law-and-ethics/legal-framework/how-legal-sources-interact [Accessed 27 June 2016]

data, but policies are targeted at different audiences (institution administrators on the one hand, researchers on the other) and so do not map on to one another.

2.2 Research misconduct, good research practice and research integrity

Where no reference is made to the legislative framework for managing and protecting data, relevant research policies are vague and/or non-transparent with regard to current sanctions for data misuse. One complexity of identifying whether sanctions exist is that such provisions may exist in different policies. Few organisations (with the exceptions noted above) have policies that set out sanctions for misuse of personal data specifically. It is more common that this kind of behaviour would fall under broader policies on research misconduct – with reactive sanctions that punish instances of wrongdoing – or be considered failures of standards of good research practice or research integrity.

The majority of policies currently in operation do not distinguish between different types of behaviour that could be subject to sanctions or how granular the specification of 'misuse' or misconduct in relation to data should be. This means there is often no one clear, authoritative resource for each organisation that sets out what the sanctions could be, for what kind of breach, and how these will be handled in each case.

Given the paucity of detail in existing policies, we have set out the distinctions below on the basis of an assumption that 'misuse' would tend to refer to a specific incident in which data protection law or the terms of an agreed contract may have been broken. We have taken 'misconduct' to refer to sets of behaviours that funders or oversight bodies would deem ethically unacceptable but that perhaps do not breach legal or contractual obligations.

Instances of misconduct:

- Data hoarding (unreasonable or unjustified withholding of data);
- Provision of inaccurate or incomplete data or information (e.g., in data submission, access application, or progress report); or inaccurate information about data (ownership, copyright, consent etc)
- Failure to appropriately acknowledge the efforts of contributors;
- Failure to respect benefit sharing requirements;
- Non-communication of research impact.

Instances of misuse:

- Data misuse (non-compliance with applicable laws, regulations, guidelines, policies, approved protocol, or access agreements); breach of information security procedures
- Data breach (the wrongful release of data, whether as a result of accident, negligence or malice); contained or uncontained breach. This would include deliberate attempts to re-identify individuals.

2.2.1 Policies relating to misconduct

All funders, research resources and repositories included in the scoping have policies on research misconduct in general. The Research Councils make specific reference to issues concerning confidentiality and identity disclosure in their definitions of misconduct, but do not tie these to obligations under the DPA:

- MRC: 'disclosing improperly the identity of individuals or groups involved in research'

- ESRC: ‘confidential nature of information…should be respected’
- RCUK: ‘improperly disclosing identities’

The Concordat on Research Integrity[19] (to which the Research Councils and Wellcome Trust are signatories) also refers to breaches of confidentiality and misuse of personal data as failures to meet ethical, legal and professional obligations.

Table 2 provides details of research funder/body policies that stipulate what sanctions are available for those who are found to be guilty of research misconduct. Note that there may be many other routes that funders could take to influence or punish poor behaviour either formally or informally, but the focus here is on stated policy with sanctions that could be applicable to instances of data misuse.

Funder/ Research Body	**Type of Sanction**							
	Warning	**Employment**	**Financial**	**Criminal**	**Publishing**	**Access to data**	**Funding withdrawal**	**Other**
RCUK							From individual. Stop considering grants from individual	
CRUK		Removal from a particular project			Retraction of published material		Termination of grant	
Wellcome	Letter of reprimand	Changes to staffing of a particular project			Withdrawal of published material			Discussion with host institution on appropriate sanctions
MRC	Final written warning	Removal from a project	Removal of eligibility for pay progression				Withdrawal of funding for program	
ESRC							Immediate suspension of project/ halt to new proposals from institution	

Table 2: Research funder policies on sanctions for research misconduct

Funders commonly consider it the responsibility of the researcher’s institution to investigate and apply penalties for misconduct. They state that institutions should notify the funder if the allegation is upheld. In exceptional cases, including systematic failures across an organisation or possible inappropriate handling of an allegation of misconduct, the funder may conduct its own investigation.

Several research misconduct/integrity policies include a statement that sanctions will not be applied in cases of inadvertent errors in data use, when no intentional deception was planned and/or when breaches are self-reported.

[19] http://www.universitiesuk.ac.uk/policy-and-analysis/reports/Pages/research-concordat.aspx [Accessed 11 May 2016]

The publishers examined do not have specific policies relating to data misuse, but PLOS and The Lancet indicate they are signatories of the Committee on Publication Ethics (COPE) Code of Conduct, which includes clauses on protecting individual data and pursuing proven instances of research misconduct. Of the six publishers investigated, only one lists sanctions for research misconduct, but several provide general statements of principles of research integrity. Publishing sanctions outlined for general research misconduct include:

- Informing the author's institution.
- Retraction of published articles.
- Refusal to consider future work from authors for a given time.

2.2.2 Data Access/Material Transfer Agreements and User Licenses

Sanctions for misuse of data tend to be specified in the terms of Data Access Agreements (DAA), Material Transfer Agreements (MTA), or data use licenses, rather than in funder policies. These agreements are made between the data controller (usually a research institution or repository) and an applicant who wishes to use research data or samples. Sanctions may be imposed if data users breach the terms of these agreements. Breaches may not necessarily involve misuses of personal data, but may capture deliberate attempts to circumvent prescribed processes and policies for handling data.

Agreements and licences used by repositories standardly indicate that the penalty for breaching the terms of the agreement is that access to data/samples will be revoked, for a particular period of time depending on the severity of the breach. Sanctions can be targeted at the individual user or at their institution. Breaches are generally investigated by the repository or administrator organisation, which also determines and imposes the sanctions. Bodies such as the ADRN make explicit reference to the DPA but in general it is not specified whether or not there is a legislative basis for sanctions if data is misused.

Regarding data misuse, most DAAs only specify the need to report any breaches of the agreement to the relevant authorities:

- The UK Data Service specifies that breaching of its End User License[20] will lead to removal of data access privileges while the breach is investigated. It goes on to describe possible legal action, though it makes no reference to specific legislation.
- UK Biobank MTA[21] requires that any inadvertent identification of a participant is reported to the UK Biobank immediately.
- The Database of Genome and Phenotypes also requires that any breaches of data security are reported to the data access controller within 24 hours. No further description of sanctions is provided.
- The *Data.bris* (Bristol Universities data repository) DAA[22] specifies the need to report any unauthorised use of the data in the repository.

[20] https://www.ukdataservice.ac.uk/media/455131/cd137-enduserlicence.pdf [Accessed 27 June 2016]
[21] http://www.ukbiobank.ac.uk/wp-content/uploads/2011/11/Access_Procedures_Nov_2011.pdf [Accessed 1 August 2016]
[22] https://data.bris.ac.uk/sensitive-research-data/ [Accessed 12 September 2016]

It is unknown whether these agreements are routinely audited or sanctions for breaches enforced, so it is not possible to assess the effectiveness of these agreements in ensuring data misuse does not occur.

2.2.3 'Proactive' policies

A more nuanced approach to sanctions has been taken by several organisations. These aim to be proactive in preventing data breaches by addressing risks and poor processes rather than only reacting when breaches occur.

Typical instances of poor researcher behaviour that could be covered by these policies include attempting to bypass rules and protocols about data access and management that are perceived as obstacles or inconveniences for research. For example, downloading data onto a USB stick to work on at home; passing data on to a colleague for their advice or input into a scientific question; or experimentally linking datasets to check for gaps in the data: all of these actions may be undertaken with the intent of doing better science, but could technically breach the terms of data use or otherwise increase the risk of a breach arising.

'Proactive' policies consider sanctions for data misuse or misconduct as part of a broader framework that aim to create a culture of responsibility for research practice rather than reluctant compliance with funder or institutional policies. The ADRN and the GA4GH accountability policy provide the most detail on the circumstances under which sanctions should apply.

- The Global Alliance for Genomics and Health has recently developed an 'accountability policy', which couches sanctions for data misuse (among other forms of non-compliance with the policy) within a broader governance framework. This is designed to improve the transparency and accountability of research practice in the field of genomics.
    - The policy adopts a 'networking' approach, recognising that full accountability for how data is used and managed requires a network of different stakeholders to act together and each be clear on what responsibility they have.
    - It provides guidance directed at stakeholder responsible for oversight of data sharing. It outlines best practices for monitoring and responding to non-compliance with data sharing standards. The policy also notes that repeated episodes of non-compliance may warrant sanctions for an entire institution.
    - The sanctions for non-compliance include:
        - warning;
        - compliance audit;
        - suspension of employment/ access/ funding;
        - retraction of publications;
        - reports of non-compliance to data stewards/ donors; employer of the data user; regulatory authorities or law enforcement officials.
    - The scoping work carried out did not reveal any example policies from the members of the Global Alliance for Genomics and Health that have yet implemented this approach.

- Genomics England is adopting a 'health and safety' approach to data use, to encourage a culture of responsibility. Such an approach encourages near misses or accidents to be reported and learned from, for example by adapting processes to mitigate the risk of human error resulting in a data breach.

- The ADRN takes an 'information security' approach that is similarly based on a learning culture: it is encouraged that mistakes or accidents are reported and in most instances if no intentional breach occurs, the repercussions for the individual or organisation will involve further training or modification of processes to mitigate future risk.
  - The sanctions policy reflects this approach, with penalties listed for 'security incidents' including breaches of information security procedures, as well as for actual instances of data breaches.
  - Sanctions for individuals include:
    - official warning;
    - suspension of access to ADRN services until individual undertakes retraining;
    - suspension of access to ADRN services for a specified time (1mo to 2+ yrs);
    - notification of breach to other data services;
    - sanction from funders;
  - Breaches by organisations attract sanctions including:
    - Suspension of access to services (6 months to 5 years)
    - Sanction from funders

2.2.4 The SURE approach

SURE (Safe Use of Research Environments)[23] training has been developed by the UK Data Service to deliver the ONS approved researcher accreditation. Part of this process will be to develop a 'researcher passport' such that accredited status could be transferred across different contexts and mitigate the need for researchers to repeatedly demonstrate their credentials to access different datasets. One implication of this approach could be that sanctions could also be portable, i.e. is a researcher misuses data in one context this could be flagged when they seek to apply data in another.

3. The role of sanctions for funders

There has been increasing political interest in the use of sanctions to deter and punish misuse of data, but it is not yet clear whether and how such sanctions will be implemented into UK law. The current legal framework for the use of personal data is at best confusing for researchers and institutions, and may also not be fit for purpose as new data technologies and data science techniques develop. It is difficult to identify what sanctions could be imposed if personal data is misused, by whom, and through what process.

This difficulty is compounded in research because of the grey area between personal and non-personal data that is not well-defined. Whether data used by researchers constitutes

[23] http://blog.ukdataservice.ac.uk/a-new-integrated-approach-training-researchers-to-use-sensitive-microdata/

personal data, and therefore falls within or out of scope of the legal framework on data use, may shift depending on its use environment and the technologies and techniques available. As the DPA applies only to personal data, a person would not commit an offence if they deliberately attempted but failed to successfully re-identify an individual from a dataset.

There are three different bases upon which to impose sanctions:

- Legal – breach of the law relating to use of personal information;
- Contractual/policy – breach of contract/license; failure to adhere to terms and conditions;
- Ethical/good practice – failure to meet standards of established good practice; using poor processes that increase risk of misuse/a breach

At present the majority of funder policies only make provision for legal and contractual or policy based sanctions, with investigations of misuse devolved to research institutions. Failures to meet standards of ethical or good practice do not, from the evidence gathered, attract sanctions from any of the EAGDA funders.

Annex 1: Definitions and terms

The vocabulary used to describe personal data, its governance and what responsibilities people have towards data is often confusing and inconsistent. Below the terms most relevant to this report are set out as defined in law.

Data Protection Act terms

Data controller: A person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed. Even if an individual is given responsibility for data protection in an organisation, they will be acting on behalf of the organisation, which will be the data controller. The term is used jointly where two or more persons (usually organisations) act together to decide the purpose and manner of any data processing. The term in common applies where two or more persons share a pool of personal data that they process independently of each other. Legal responsibility for compliance under the DPA falls on the data controller[24]

Data processor: A person/organisation who processes the data on behalf of the data controller. Processing refers to obtaining, recording or holding the information or data or carrying out any set of operations on the information or data.

Personal Data: Data which relate to a living individual who can be identified – (a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Data Misuse: (a) the processing of those data or their processing for that purpose or in that manner is causing or is likely to cause substantial damage or substantial distress to him or to another, and (b) that damage or distress is or would be unwarranted.

EU GDPR terms

Personal Data: Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

Data Misuse: There are extensive definitions and provisions for the different infringements of the Regulation and the sanctions that such actions are subject to. These include infringements of:
(a) the basic principles for processing, including conditions for consent […];
(b) the data subjects' rights […];
(c) the transfers of personal data to a recipient in a third country or an international organisation […];
(d) any obligations pursuant to Member State law […];

[24] https://ico.org.uk/media/1546/data-controllers-and-data-processors-dp-guidance.pdf para. 56 [Accessed 22 June 2016]

(e) non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority […] or failure to provide access […].

Statistics and Registration Services Act

Personal Information: Information which relates to and identifies a particular person (including a body corporate); but it does not include information about the internal administrative arrangements of the Board (whether relating to its members, employees or other persons).

Data Misuse: Personal information held by the Board in relation to the exercise of any of its functions must not be disclosed by – (a) any member or employee of the Board, (b) a member of any committee of the Board, or (c) any other person who has received it directly or indirectly from the Board.

Digital Economy Bill

Personal information: Information is "personal information" if – (a) it relates to and identifies a particular person (including a body corporate), but (b) it is not information about the internal administrative arrangements of a specified person.

Data Misuse: Same definition as DPA plus additionally:
(5) A person who contravenes subsection (2) is guilty of an offence
(2) (2) Personal information to which this section applies may not be disclosed—
(a) by P, or
(b) by any other person who has received it directly or indirectly from P.