Data Protection & Research:

Guidance for MRS Members and Company Partners 2019

Table of Contents

Section 1:
Introduction

This section discusses the purpose and structure of this MRS Data Protection Guidance 2019, developed through informal consultation with the ICO. It also defines key data protection terms.

1.1 Purpose and scope

Regulatory guidance is integral to effective compliance with the data protection framework introduced by the UK Data Protection Act 2018 (DPA 2018)[1] and the EU General Data Protection Regulation 2016 (GDPR)[2]. This Guidance, for MRS members and Company Partners, was developed through informal consultation with the Information Commissioner's Office (ICO).

The purpose of this document is to provide guidance to assist researchers understanding of and compliance with the requirements of the GDPR and the DPA 2018. This data protection legislation works with the provisions in the MRS Code of Conduct to provide an overarching ethical and legal framework for research.[3]

The MRS Code of Conduct requires that research conforms to national data protection legislation. This document sets out the expectations of MRS on the application of data protection rules in a research context. The Guidance will be taken into account in determining whether there has been a breach of the Code.

Market research, which includes social and opinion research, is the systematic gathering and interpretation of information about individuals or organisations using the statistical and analytical methods and techniques of the applied social sciences to gain insight or support decision making. Research itself does not seek to change or influence opinions or behaviour and is not used to take decisions or actions regarding a specific individual. The approach in this Guidance differs from earlier MRS Data Protection Guidance which places data collection projects into different categories (Categories 1 to 6), to differentiate the boundaries between classic research and projects conducted for other purposes. In the new guidance this has been replaced by a primary distinction between research and non-research.

This document replaces the MRS Data Protection & Research Guidance 2018 and reflects current published ICO guidance. It will be periodically updated in line with data protection guidance and any additional clarifications issued by the UK ICO and the group of EU regulators, the European Data Protection Board (EDPB). There is also a supplementary series of subject specific guidance notes covering areas available on the MRS website at https://www.mrs.org.uk/standards/legislation/tab/data_protection.

MRS is providing this data protection guidance as general information for research practitioners. It is not legal advice and should not be relied upon as such. Specific legal advice should be taken in relation to any specific legal problems or matters.

[1] The DPA 2018 can be found here: http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted
[2] The GDPR can be found here: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=en
[3] The MRS Code of Conduct can be found here: https://www.mrs.org.uk/pdf/mrs%20code%20of%20conduct%202014.pdf

1.2 Structure

This Guidance document is divided into five sections which provide a general overview of the specific topic area, highlight the key points and discuss the application to research data collection and processing exercises.

It discusses core data protection principles and concepts as well as the legal grounds for processing personal data in the context of research activities. Members should also consult the stand-alone MRS data protection guidance for additional information on specific topics.

1.3 Key terms

The key terms in the GDPR have the same meaning in the DPA 2018. Any modifications or exceptions from this are highlighted in the text of this Guidance document.

Anonymous Data

Anonymous data is "information which does not relate to an identified or identifiable natural person or to data rendered anonymous in such a way that the data subject is not or no longer identifiable." Anonymous data is no longer personal data, and the data protection rules do not apply. It is increasingly difficult to properly anonymise personal data. Focus is generally placed not on the absolute impossibility of identification but the likelihood of re-identification occurring. In determining whether the data has been anonymised consideration must be given to "all the reasonable means likely to be used" taking into account factors such as cost, available technology and amount of time. (Recital 26 GDPR)

Data Controller

Data controllers determine the purposes and means of the processing of personal data. The concept of joint data controllers is formally recognised in the GDPR and applies where controllers jointly determine the purposes and means. (Article 4 GDPR)

Organisations must understand whether they are acting as a data controller or data processor on a project in order to determine which specific legal obligations under the GDPR are applicable and to reflect these in the contract between parties.

Data Processor

Data processors process personal data on behalf of controller(s). In a research context an organisation is likely to be a data processor where it is processing personal data solely on the client's behalf such as transcription, processing, coding, analysing and translation activities. (Article 4 GDPR)

Data Protection Impact Assessment (DPIA)

DPIA is a process designed to help organisations identify and mitigate data protection risks of a project. (Article 35 GDPR) Certain high risk processing activities require that a DPIA is carried out. ICO has issued a list that is available here https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/examples-of-processing-likely-to-result-in-high-risk/

Data Subjects

Data subjects are identified or identifiable living indivduals to whom the personal data that is held relates. (Recital 26 GDPR)

Personal Data

Personal data is information relating to an identified or identifiable natural person; who can be identified directly or indirectly by that data on its own or together with other data. This includes identifiers such as a name, an identification number, location data, device identifiers, cookie IDs, IP addresses and relates to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

To determine whether a person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by a data controller or by any other person to identify an individual directly or indirectly. (Article 4 GDPR)

Personal data breach

Personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. (Article 4 (12) GDPR)

Processing

Processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. (Article 4(2) GDPR)

Profiling

Profiling means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. (Article 4(4) GDPR)

Pseudonymisation

Pseudonymisation is the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person. (Article 4(5) GDPR)

Special Category Data (previously referred to as Sensitive Personal Data)

Personal data categorised as special category data is data on:

- religious or philosophical beliefs
- health
- racial or ethnic origin
- trade union membership
- political beliefs
- sex life or sexual orientation
- genetic data
- biometric data (including photos when used for the purpose of uniquely identifying a natural person) of data subjects. (Article 9 GDPR; Sched. 1 DPA)

The collection and use of special category data is subject to greater restrictions than other types of personal data particularly regarding additional legal grounds for processing and considerations of risk in processing of personal data.

Personal data relating to **criminal convictions and offences** is not included in special category data, but extra safeguards also apply to processing this data. (Article 10 GDPR; Sched. 1 DPA)

Research

Research is the collection, use, or analysis of information about individuals or organisations intended to establish facts, acquire knowledge or reach conclusions. (MRS Code of Conduct)

Scientific research

Scientific research is not defined in the GDPR but the GDPR makes it clear that scientific research purposes should be interpreted in a broad manner, including for example technological development and demonstration, fundamental research, applied research and privately funded research. Scientific research will include both privately and publically funded research that is set up and conducted in line with relevant appropriate methodological and recognised ethical standards. Additionally, the DPA 2018 makes it clear that scientific research must be carried out in the public interest in order to be used as a processing ground for special category data. (Recital 159 GDPR; Section 18 DPA 2018)

Statistical research

Statistical research is not defined in the GDPR but statistical research purposes are "any operation of collection and processing of personal data necessary for statistical surveys or for the production of statistical results." Research that results in aggregate data that is not used to support measures or decisions regarding an individual is statistical research. The outputs of statistical research can also be further used for other purposes including scientific research. (Recital 162 GDPR; Section 18 DPA 2018)

Section 2:
Overview

This section provides an overview of the relationship between the GDPR and the UK Data Protection Act 2018 and explains significant changes in key data protection concepts.

2.1 Relationship between GDPR and DPA 2018

The General Data Protection Regulation (GDPR) came into effect in all EU Member States on 25 May 2018. It is directly applicable in all EU Member States without any further implementing domestic law.

After the UK formally leaves the European Union, the national data protection framework, will continue to reflect the GDPR, but will be applied in the manner set out in the UK Data Protection Act 2018 (DPA 2018). In addition to restating the provisions of the GDPR, the DPA 2018 also sets out tailored national exemptions (in areas allowable under the GDPR) and provides a legal framework for data protection in criminal justice and law enforcement. It also replaces the Data Protection Act 1998 (DPA 1998).

Additionally, withdrawal of the UK from the EU will have other data protection implications including the fact that the UK will become a third country and the extra territorial provisions in the GDPR will apply in the UK. The MRS series Brexit and Research provides additional guidance in this area.

In this Guidance references to the GDPR should be interpreted as references to the GDPR as implemented by the DPA 2018. References are made to the articles of GDPR and sections of the DPA 2018 as appropriate. The Guidance reflects the UK national implementation of the GDPR and differences in the data protection framework as a result of specific national rules in the UK implementing legislation are generally highlighted in the text.

2.2 New and significantly changed concepts between DPA 1998 and GDPR/DPA 2018

The GDPR introduced new concepts and rules and significantly changed core provisions in the previous data protection framework. The changes of greatest relevance to researchers are:-

- **Wider definition of personal data** – The GDPR expands on the definition of personal data in the DPA 1998 to explicitly acknowledge that online identifiers such as cookies and similar technology such as IP addresses can be personal data.[4] It also expands the category of special category data (previously known as sensitive personal data) to include sexual orientation, biometric data used for identification purposes and genetic data.
- **New concepts of accountability and data protection by design and default** – Data controllers are accountable and must be able to demonstrate compliance with the data protection principles and

[4] The text in a cookie often consists of a string of numbers and letters that uniquely identifies a computer, but it can contain other information as well. Cookies are often used by web pages to help users navigate their websites efficiently and perform certain functions within pages or logins.

use appropriate organisational and technical measures to ensure compliance. Additionally, the concept of data protection by design and default requires data controllers to ensure that data subjects' privacy is considered from the outset of each new processing, activity or development of new products, services or applications. It also means that, by default, only the minimum amounts of personal data as necessary for specific purposes are collected and processed. This also means that techniques such as pseudonymisation must be effectively utilised.

- **Statutory liability of data processors** - Data processors and data controllers are both directly liable through statutory obligations in contrast to the previous regime which placed liability only on data controllers. Data processors are jointly and severally liable with data controllers for compensation claims from data subjects.
- **Mandatory appointment of Data Protection Officer (DPO)** – DPOs are mandatory in certain circumstances. DPOs are required for public bodies, and for organisations whose core activities either require regular and systematic monitoring of data subjects on a large scale or involve large scale processing of special category data and data relating to criminal convictions. Appointment of a DPO is likely to be a requirement for most research suppliers.
- **Higher standard of consent** –GDPR requires unambiguous consent that is freely-given, specific, informed and evidenced by clear affirmative action or statement (silence or pre-ticked boxes are not evidence of consent). Consent must also be verifiable with higher standard of explicit consent required to process special category data.
- **Mandatory notification of personal data breaches** – Data breaches must be notified to the ICO without undue delay and within 72 hours of becoming aware of the breach where there is a likelihood of risk to data subjects. Notification must also be made to affected data subjects where there is a high risk the data breach is likely to cause harm.
- **Territorial scope**– The GDPR applies to organisations outside the EU who are offering goods or services to or monitoring data subjects resident in the EU. These organisations will generally need to appoint a representative based in the EU. In light of this, it is also important to note that when the UK is no longer a member of the EU, UK-based organisations monitoring EU citizens will be subject to the GDPR and any tailored national provisions in individual Member States.

For further information see:

- MRS: Brexit and Research: Appointment of EU representative
- MRS: Brexit and research: EU-UK Data Transfers
- MRS: Brexit and research: EU-UK Data Transfers Standard Contractual Clauses
- MRS: GDPR In Brief (No.1): Changes in UK Data Protection Framework (Member Content)
- ICO: Guide to the GDPR

Section 3:
Data Protection Principles and Concepts

This section discusses the data protection principles and key new concepts of accountability, data protection by design and default and pseudonymisation. It explains how these principles should be embedded through the research cycle.

3.1 Data protection principles

The GDPR, sets out six data protection principles, which largely cover the eight data protection principles set out in the DPA 1998:

- **Lawfulness, fairness and transparency** – Personal data must be processed lawfully, fairly and in a transparent manner.
- **Purpose limitation** – Personal data must be obtained for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing is allowed for archiving, scientific, statistical and historical research purposes.
- **Data minimisation** – Personal data processed must be adequate, relevant and limited to what is necessary.
- **Accuracy** – Personal data must be accurate and, where necessary, kept up to date.
- **Storage limitation –** Personal data must not be kept longer than is necessary (but data processed for archiving, scientific, statistical and historical research purposes can be kept longer subject to safeguards).
- **Integrity and confidentiality** – Appropriate technical and organisational measures must be put in place to guard against unauthorised or unlawful processing, loss, damage or destruction.

3.2 Data protection concepts

The new concepts of accountability, data protection by design and default and pseudonymisation work with the data protection principles to underpin the new legislation.

Accountability

Accountability requires that data controllers and data processors are responsible for, and are able to demonstrate compliance with the data protection principles. It requires research organisations to put in place appropriate technical and organisational measures and to be able to demonstrate what they did and its effectiveness.

Accountability measures include:

- Use of data protection impact assessments for high risk processing
- Appropriate documentation including internal records of processing activities
- Mandatory data breach notification regime
- Appointment of data protection officer

Data mapping, the process of identifying, understanding and mapping out the data flows of an organisation is a valuable process to support privacy compliance and underpin accountability. Data flows may vary project by project.

Data protection by design and default

Data protection by design and default means that all data collection exercises must be proactively designed and conceptualised in the most privacy enhancing way. This needs to be done by embedding privacy in organisational practices, policies and procedures and can include:

- Limiting access to personal data– Ensure that only those who need access to data are granted access privileges.
- Minimising data collection – Limit data collection to the data required for the research project/exercise.
- Retaining personal data for reasonable but generally short periods – establish appropriate retention period(s), advise clients as to what the retention period is and periodically review and revise limits.

Alongside these organisational processes, technical safeguards and design systems of any IT architecture need to embed privacy. This must include data protection impact assessments (DPIA's) for applicable projects. DPIAs have a vital role to play in any GDPR compliance programme as they allow identification of potential privacy issues at an earlier and less costly stage. They also reduce the risks and increase of awareness of privacy and data protection with staff members throughout organisations.

In implementing data protection by design the GDPR requires that data controller(s) take into account several factors:

- the state of the art (which varies over time and is based on constantly evolving best practices and technology)
- the cost of implementation
- the nature, scope, context and purposes of processing
- the likelihood and severity of risks to the rights and freedoms of natural persons posed by the processing of their personal data

This means that organisations can take a flexible risk based approach, the higher the risk, the more rigorous the measures that must be taken and as with other compliance obligations under the GDPR it will be key to ensure this is documented.

Pseudonymisation

Pseudonymisation of personal data is highly encouraged in processing data for research purposes. It is the processing of personal data so that it can no longer be attributed to a specific data subject without the use of additional information, such as a unique identifier, which can make the data identifiable. Although pseudonymised data is still personal data, it is a useful data security measure that can limit an organisation's risk profile and exposure for personal data breaches.

In order to become pseudonymised data, the unique identifier must be kept separately and held subject to adequate technical and organisational measures. Data can be considered as pseudonymised even where the unique identifier is kept within the same organisation. If the holder of the pseudonymised data does not have the means to reverse or unlock the pseudonymisation, then the data that they hold will be anonymised rather than pseudonymised data. The difference between pseudonymised and anonymised data is that for anonymised data there exists no key to link the data to the individual.

Although pseudonymised data may sometimes also be referred to as de-identified data, this is not a term that is used in the GDPR.

3.3 Data subject rights

The GDPR incorporates rights and protections for data subjects participating in research such as the ability to access their data or require it to be rectified or deleted. In certain circumstances data subjects will also be able to request that their data is ported to another organisation and object to processing of the personal data.

The application of these rights is discussed in Table 1.

Table 1: Individual rights under GDPR/DPA 2018

Right	What does this mean?	Are there limits to this right?
Right to be informed	Right to be provided with extensive information including on all their rights, contact details, source, retention period, purposes, categories and recipients etc.	If the information is not collected directly from data subjects and providing the privacy information would be impossible, or would involve a disproportionate effort then the right can be limited. However this is a core transparency requirement so any limitations will be interpreted narrowly. Additional exceptions also apply.
Right of access	Right to access personal data within 30 days and for free. It must be possible to make electronic subject access requests.	Data can be withheld if disclosure would adversely affect the rights and freedoms of other data subjects.
Right to rectification (of inaccurate data)	Right to have inaccurate records corrected.	Organisations can refuse to comply with a request for rectification if the request is manifestly unfounded or excessive, taking into account whether the request is repetitive in nature.
Right to erasure "to be forgotten	Right to erasure of information with an obligation on the controller to inform other controllers to also delete. This is a complex right in terms of applicable situations and exemptions. It applies where individuals have objected and there are no overriding legitimate grounds to justify processing; data is no longer needed for purpose for which it was collected; consent is withdrawn and there is no other ground for processing; personal data is unlawfully processed; a legal personal data obligation; processed in connection with online service offered to a child.	Right can be restricted • in the public interest or carried out by an official authority • for archiving or research purposes • necessary for freedom of expression or information • public interest in the area of public health • fulfilment of legal claims

Table1 : (Cont'd) Rights of individuals under DPA 2018/GDPR[5]

Right	What does this mean?	Are there limits to this right?
Right to restrict processing	Right to request that processing be restricted where data cannot be deleted as it is required for legal reasons. This is a more limited right than the right of erasure. It allows controllers to quarantine data to be used solely for a limited range of purposes such as handling legal claims.	Organisations can refuse to comply with a request for restriction if the request is manifestly unfounded or excessive, taking into account whether the request is repetitive in nature.
Right to data portability	Right to request personal data be provided in usable, transferable format to allow data to move between platforms or suppliers.	This right only applies to data collected by the controller by consent or contract.
Right to object to processing	Right to object to processing that is based on processing grounds of legitimate interests or public task.	Organisations do not need to comply if processing is for legal claims or based on a compelling legitimate interest which overrides the interests of the individual. The burden of proof is on the controller to show there are compelling grounds for the continued processing.
Right to withdraw consent	Right to withdraw consent in as easy a manner as it was to give consent.	Reflection of ethical best practice for research.
Right not to be evaluated by automated decision making	Right not to be evaluated or subject to decisions where decision has legal or significant effects.	Right does not apply if the decision is based on explicit consent; necessary for a contract; authorised by Union or Member State law.

Transparency is critical and clear detailed information must be provided to research participants including information on the legal basis used to process personal data.

- Privacy notices for researchers is discussed in the MRS GDPR In Brief No. 7 Transparent Privacy Notices (Member Content)

Researchers must consider who is most appropriately placed to send out invitation letters, noting that data subjects must be provided with or referred to the applicable privacy policy/processing statement of the controller which sets out what their rights are and how they can be enforced. In certain circumstances researchers may be exempted from providing information for indirect collection of data from data subjects.

- Determination of who is the controller or the processor in a research project is discussed in the MRS Guidance Note - Controllers and Processors (Member Content)

[5] NB Other rights – rights to restrict processing, right of a child to be forgotten, right to information

A summary of the information requirements, which vary depending on whether you are collecting the data directly or indirectly from research participants is set out below in Table 2.

Table 2: Information requirements when collecting data directly or indirectly from data subjects

What information must be supplied?	Direct collection of data from data subjects	Indirect collection of data from data subjects
Identity and contact details of the controller (and where applicable, the controller's representative) and the data protection officer	✓	✓
Purpose of the processing and the legal basis for the processing	✓	✓
The legitimate interests of the controller or third party, where applicable	✓	✓
Categories of personal data		✓
Any recipient or categories of recipients of the personal data	✓	✓
Details of transfers to third country and safeguards	✓	✓
Retention period or criteria used to determine the retention period	✓	✓
The existence of each of data subject's rights	✓	✓
The right to withdraw consent at any time, where relevant	✓	✓
The right to lodge a complaint with a supervisory authority	✓	✓
The source the personal data originates from and whether it came from publicly accessible sources		✓
Whether the provision of personal data part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the personal data	✓	
The existence of automated decision making, including profiling and information about how decisions are made, the significance and the consequences.	✓	✓

When should information be provided?	At the time the data are obtained.	Within a reasonable period of obtaining the data (within one month); If data used to communicate with the individual, at the latest, when the first communication takes place; or if disclosure to another recipient is envisaged, at the latest before the data are disclosed.

3.4 Embedding data protection principles and concepts in the research cycle

The data protection principles are inter-related and researchers need to ensure that the principles are followed, as applicable, throughout the full research cycle. Principles will need to be applied by all parties within the research supply chain to ensure that sub-contractors acting as data processors adhere to the policies and processes set out by the data controller(s), who may be the client and/or the lead researcher.

Written contracts must always be used to clearly set out the roles and responsibilities of all parties within the research supply chain including the commissioning client, research agency, fieldwork agency as well as any freelance interviewers or recruiters.

This section discusses the scope and treatment of personal data in research projects and sets out general points for consideration in applying the data protection principles across the research cycle.

3.4.1 Scope of personal data in research

The scope of what constitutes personal data must be broadly construed in light of the definition of personal data in the GDPR. This relates to the possibility of identifying an individual rather than a pre-defined list of information attributes. Consideration must always be given to the means and likelihood of re-identifying individuals. Re-identification risks are dynamic and will increase in line with technological improvements and reduced costs.

Use of anonymised or pseudonymised data

It is important to consider whether and if so the earliest point in the process that personal identifiers can be removed from any data in order to create anonymised or pseudonymised datasets.

- In order to understand whether data can be anonymised it is also important for researchers to check and understand what other data research clients might have that could lead to identification of research data subjects being re-created from anonymised survey data in order to satisfy themselves that the data will remain as anonymised data upon transfer to a new environment e.g. a client's. Assurances should also be sought from the client that the data will not be matched with other data in the client's control (to create personal dataset).
- As effective anonymisation is difficult researchers must also document why and how the personal data will be "anonymised" rather than "pseudonymised". If in doubt about the effectiveness of the anonymisation researchers must treat the data as personal data (particularly if it was special category data in light of the higher level of harm if the data is re-identified).
- If data cannot be anonymised then it must, as far as feasible, be pseudonymised, in order to reduce the risks of processing.

Photographs, audio recordings and other visual images

Researchers should note that photographs, audio recordings, video recordings (such as fieldwork video footage) and still images are likely to be personal data even if the individuals are not named.

- Determination of whether these are personal data will depend on context. However, the ease of technology in linking these to an identifiable person means that there is a higher risk of re-identification for this type of media. In light of this steps must be taken to anonymise this material where guarantees of participant anonymity have been made as part of the research project.
- In order to properly anonymise audio and video recordings, transcripts of recordings can be used,

ensuring that these transcripts are edited to remove any comments that may lead to identification of a data subject in the research study. Pixelating or blurring images can also be used to anonymise or pseudonymise images. Please note that although photographs are generally personal data they will also be special category data where technical processing is used to allow the photos to uniquely identify a natural person such as in an electronic passport.

Observed, inferred or derived data

Personal details or characteristics inferred or derived about data subjects from the analysis of data provided, rather than data provided directly by them, must also be treated as personal data or special category data as applicable.

- Observed data (such as online cookies automatically recorded), derived data (such as data produced from using other datasets) or inferred data (such as using algorithms to predict health outcomes based on combining information in different datasets) produced during analysis of data may trigger different privacy risks than traditionally provided data. These risks must be considered in assessing privacy implications of the research project.
- If special category data is inferred as a result of profiling, the controller needs to make sure that the processing is not incompatible with the original purpose; there is a lawful basis for the processing of the special category data and data subject has been informed about the processing. Researchers must ensure there is a processing condition for processing any special category data where undertaking this type of project.

Figure 1: Research Cycle

3.4.2 Scoping or setting-up research project

Researchers designing or setting up a data collection exercise must ensure that consideration is given to designing the research in such a way that the amount of personal data collected is only that which is necessary to meet the research objectives.

Research proposal

The submission of a research proposal to a client should include, where feasible:

- a data management plan that sets out the key data protection and privacy issues;
- suggestions for addressing any privacy issues and/or the necessity of a Data Protection Impact Assessments (DPIA) (previously known as a Privacy Impact Assessment (PIA)).

A DPIA, carried out by a controller, is only required when processing is likely to result in a high risk to the rights and freedoms of individuals. In these circumstances, it will be necessary for the controller to assess the risks and potential harm to data subjects such as where a project involves large scale collection of special category personal data or matching of datasets collected by different data controllers in a way that would exceed the reasonable expectations of individuals. DPIAs that identify high risk data collection exercises with risks that cannot be reduced or adequately mitigated by data controller(s) will require prior consultation with the ICO in line with published ICO timeframes.

Written contract

Researchers processing personal data must always enter into a written contract that reflects the agreement between the parties. This should reflect commercial terms and conditions and must contain all mandatory GDPR requirements (if acting as controller or processor) and allocation of responsibilities (if acting as a joint controller). Contracts are also required with any sub-processors.

Determination of roles as controller or processor

Researchers must be clear as to the role that each party plays in the research project. The determination of who is a controller, joint controller, processor or third party is a question of fact rather than contractual stipulation. This means that it is based on an evaluation of who determines the purposes (the why) and the means (the how) of the processing, and essentially the level of decision-making power exercised. Parties need to review the facts and evidence for the particular processing activity, reach a decision on the roles and reflect this in the contract.

- The rationale for determination of roles, may differ on a case-by-case basis, and in these situations researchers should fully and properly document the factors taken into account in determining roles. The research project files must provide sufficient evidence to support the determinations made including details of the client brief, supplier proposal, data collection instruments, transparency and risk tools and contract.

For many research relationships the end-client will be the data controller and the full-service agency plus any subcontractors used by the research agency will be the data processor(s). In some cases, research suppliers may be joint data controller with the end-client. It is important to note that the end client may still be a data controller even if they do not themselves process any personal data e.g. receive identifiable personal data back from the research supplier. The determining factor is whether the supplier and end-client are jointly "determining the purposes and means" of processing the personal data. The contract between the parties must set out the roles of each party to the contract. However, determination as to who is a data controller or a data processor is a question of fact.

Useful ICO Guidance on the difference between data controllers and data processors and the governance implications is available here.

Naming the controllers

Under the GDPR it is a requirement that data controller(s) are named at the time the personal data is obtained.

MRS is aware that a requirement to name the end-client upfront at the start of a research exercise such as a survey may have significant consequences in certain research projects such as:

- spontaneous awareness research (assessing whether participants can quote/recall a brand name without prompting); or
- reducing methodological rigour including biasing responses where the client's identity is known up front or adversely impacting on trend data where attitudes on behaviour etc are measured over time, as the results will not be comparable.

MRS interprets the requirements in the GDPR on naming the data controller as providing some leeway on the point in time that the controller must be named. It is important that the data controller is named as part of the single process of collecting personal data, but this may be more appropriately done at the end rather than at the beginning of a survey. This may be appropriate in those circumstances where researchers, in their documented professional judgement, consider that it will adversely impact the rigour and robustness of the research to name clients at the start of a survey the data controller client must be named at an alternative appropriate point in a data collection exercise subject to the following:-

- it must be made clear to data subjects that the data controller will be named at the end of the data collection exercise; and
- assurances must be provided to data subjects that any personal data collected will be deleted if at the point that the data controller is revealed they object, wish to withdraw their consent and/or no longer wish to participate.

This approach is most appropriate when no personal data is being shared with the end client, but researchers may also consider using it in other circumstances.

If a commissioning client is a controller then in accordance with Article 13 of the GDPR they must be named "at the time the personal data is obtained." Different views have been expressed as to whether this requires the client to be named at the beginning of the data collection exercise (such as an interview) or allows some measure of discretion for the client to be named at the end before data collection processing fully starts. Note: *The more broadly that this requirement is interpreted the less likely it will be that the processing is transparent.*

It is also important to note that-

- if client is the source of the personal data then they will also need to be named as part of meeting data subject information requirements; or
- if client is receiving personal data from the data collection exercise, they will need to be named as a recipient of personal data.

In both cases set out above this information will need to be provided at an appropriate point in the data capture activity, which may be at the end of data collection.

MRS is liaising with the ICO to determine whether this approach is consistent with their interpretation of the provisions in the GDPR and DPA 2018. We will issue additional advice and guidance on this issue on completion of our discussions with the regulator. In light of this members should be aware that advice on this point is subject to change.

Note: The legal requirement is that a controller must be named. Compelling reasons will be required if a controller client is not named. If adopting a risk-based approach and a decision is taken to not name the controller client this must be based on robust evidence of the impact on the research and the client must

conduct a DPIA documenting and balancing all the risks and setting out safeguards to minimise any possible impact of the approach on the data subject.

Determination of legal processing ground

The legal ground that will be used to collect personal data such as consent of the data subject or the legitimate interests of the data controller in conducting the research must be determined at the outset of the project to ensure that the processing is fair, lawful and transparent and that data subject rights can be met.

- If special category data is being collected, the processing condition for the collection of this data must also be identified at the outset of the project. Specific policy documentation requirements in UK DPA 2018 that apply to the collection of special category data or criminal convictions data must always be met.

3.4.3 Collecting data

Researchers collecting personal data for a research exercise must:

- ensure the purpose of the data collection is clearly specified in an information notice (also known as a privacy notice or privacy information notice) which provides full details of all privacy information to data subjects.
- minimise the collection of personal data by only collecting data that is necessary.
- ensure that data subjects are clearly informed about expected uses of data and provided with an adequate privacy information notice. Researchers will generally share data that has been effectively anonymised. Participants must always be informed if personal data will be shared and if so, who the personal data will shared with.
- securely store and manage all data and build in security measures such as encryption or hashing of data taking into account the sensitivity of the data being collected and any risks to research data subjects.

3.4.4 Analysing data

Researchers analysing data collected for research or using existing data for research purposes must comply with the data protection principles. In particular researchers should note that:

- Personal data must only be used in accordance with privacy information notices provided to research data subjects.
- Use of aggregated data sets in quantitative projects and anonymised data in qualitative projects is preferable.
- Anonymised or pseudonymised datasets should be used as far as possible.
- Access to personal data must be limited to those researchers directly involved in the research exercise.

3.4.5 Reporting and/or publication

Personal data must not be included in research reports unless consent has been obtained from data subjects:

- Identifiable verbatim quotes from research data subjects can only be used with express consent of the data subject. Verbatims can be used without specific consent if they are anonymised (with the

removal of identifying contextual detail and personal information).

- Visual images, particularly video clips, can be used if images are pixelated and/or voices disguised. Other visual images must only be used where data subjects have been fully informed about their use and have consented. Intention to use or share the video clips and/or images on websites or social media platforms must be made clear to the data subject in seeking their consent.
- Special category data can only be included with the explicit consent of the data subject.

3.4.6 Retention and disposal

In line with the integrity and security data protection principle researchers must:

- keep personal data secure and dispose of it securely taking into account the risk-level of any data.
- store personal data in line with data retention policies.
- ensure that all parties within the research data supply chain with access to personal data e.g. data processors follow the same processes and policies.

For further information see:

- MRS Code of Conduct
- MRS GDPR In Brief (No. 5) Informed Consent (Member Content)
- MRS: Guidance on Controllers and Processors (Member Content)
- ICO Guide to the GDPR
  https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/
- See A29 WP Guidance on Automated Individual Decision-Making and Profiling (6 February 2018)

Section 4:
Data Processing Grounds and Conditions

This section discusses the GDPR processing grounds and conditions that are appropriate for use in research projects. The grounds discussed are consent of the data subject, the legitimate interests of the data controllers and contractual necessity. Illustrative examples are provided for all the grounds discussed.

4.1 Overview

A legal basis (or processing ground) must be identified before personal data can be processed. In all cases the processing must be necessary but there is no hierarchy of processing grounds and data controllers must ensure that the right legal basis is chosen for the data processing activity.

There are six different legal grounds available but "consent" of data subjects and the "legitimate interests" of the data controller or a third party are particularly relevant to the research sector. Additionally, "public task" for public sector research projects and "performance of a contract" for aspects of panel research are likely to be grounds used for research purposes.[6] These processing grounds give rise to different legal obligations and data controllers must record which legal ground is being used for the processing activity (with reasons) and detail this in internal data processing records.

Researchers processing personal data only need to have a processing ground. However processing of special category data requires a processing ground for the personal data as well as a processing condition for the special category data or criminal convictions data. Commonly used processing conditions in research projects are explicit consent and scientific research in the public interest.

In all cases research projects must be conducted transparently and organisations must provide full information to data subjects using a layered and blended approach such as by actively providing some information and making other information easily accessible and using a mix of tools such as infographics, videos, FAQ's etc. to provide access to information.

In assessing the most appropriate ground to use for data processing researchers must consider the category of data being processed, the nature of the research and the type of data controller. Figures 2, 3 and 4 illustrate how these factors must be taken into account. The grounds that can be used for personal data are set out in Figure 2, the conditions that can be used for special category data are set out in Figure 3 and the grounds that can be used for data processing by public authorities are set out in Figure 5.

[6] In particular it is important to note that the use of incentives to encourage participation in research is not a payment for time or participation and are not part of a contractual relationship with data subjects. Different arrangements may apply for panel providers.

4.1.1. Category of data being processed

Researchers processing special category data as well as personal data will need to have a legal basis for all categories of data being processed. If you are processing special category data you must have a lawful basis under Article 6 of the GDPR in addition to meeting a special condition under Article 9 of the GDPR but these grounds do not have to be linked.

Additionally, the UK DPA 2018 requires that where special category data is processed then appropriate policy documentation must be developed that can be made available to the ICO. The documentation must

- explain how the controller complies with the data protection principles,
- set out retention and erasure policies, and
- be kept for at least 6 months after cessation of processing.

4.1.2. Nature of research being carried out

The choice of processing ground will also be determined by the type of research (such as whether it is possible to get informed consent) or if the research is for scientific, historical or statistical research purposes or in the public interest.

Under the DPA 2018, scientific or statistical research by private sector, public sector, third sector or academic bodies that is in the public interest can use the scientific research regime as a processing condition for special category or criminal convictions data The regime for scientific or statistical research carried out in the public interest are further detailed in section 5 of this Guidance and in separate guidance (MRS/SRA Public Interest Research Guidance forthcoming Summer 2019).

4.1.3. Type of data controller

Public authorities cannot generally rely on legitimate interests as a processing ground for research activities. In this case the most relevant legal basis is likely to be processing "in the public interest". However, the standards for use of legitimate interests and public interest will be similar, requiring a balancing of the interests of the data controller and the data subject.

For further information see:

- ICO Guide to the GDPR
  https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/
- ICO Privacy Notice Guide https://ico.org.uk/global/privacy-notice/

Figure 2: Personal data processing grounds for research (Article 6 GDPR; Section 7 DPA 2018)

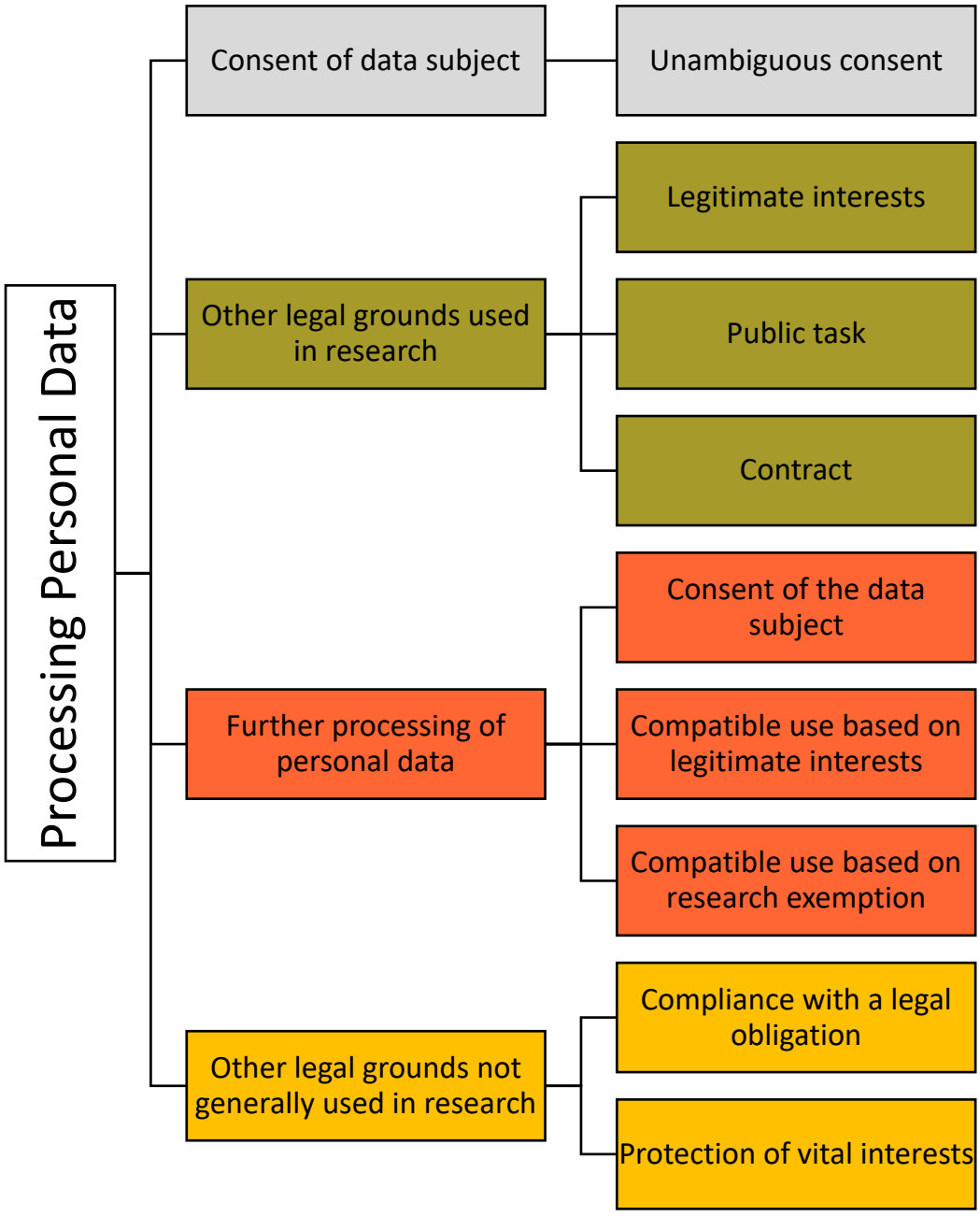
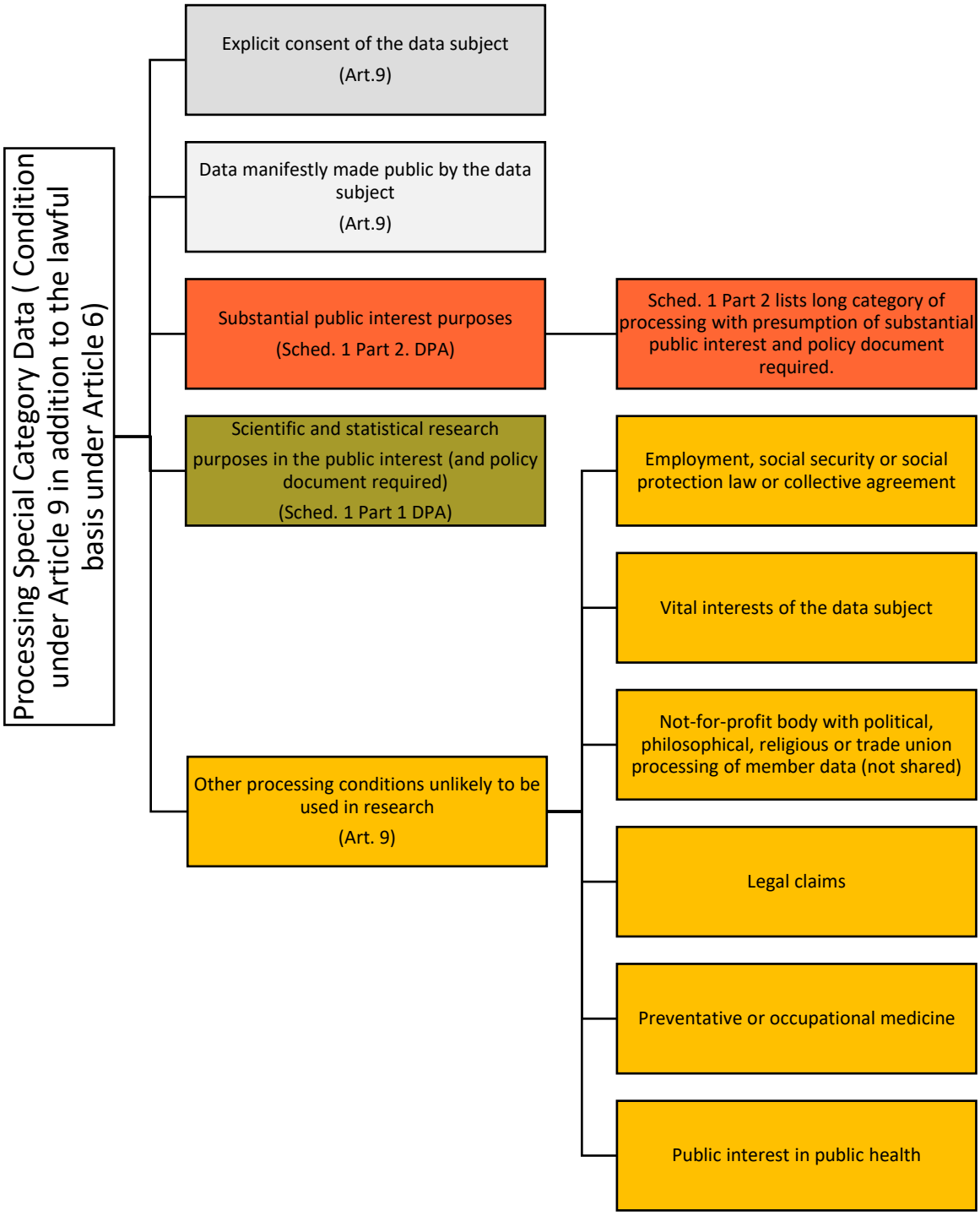


Figure 3: Special category data processing conditions for research (Article 9 GDPR; Section 9 & Sched. 1 DPA 2018)



4.2 Consent

In the research context consent has traditionally been used for a wide range of data collection exercises. Obtaining consent of data subjects in line with the GDPR is more challenging than previously as the requirements are more detailed and robust than the requirements in the DPA 1998.

Consent is essentially about individual choice and control, and although it will often be the right lawful basis for carrying out research, researchers must be certain that consent is the most appropriate ground for any research project. In considering whether consent is an appropriate ground issues such as whether the data subject can participate without consent; if they will suffer detriment as a result of refusing consent and whether consent can be withdrawn easily need to be considered.

Researchers should note that even where they are not using consent as their legal basis, they are expected to proceed in line with good research practice and high levels of transparency in their research projects. In instances, where research projects are based on other legal grounds such as public task or legitimate interests, researchers should seek to promote transparency by a range of techniques including gaining "ethical permission" which seeks to ensure that the research participant has an understanding of the research and its risks. This ethical permission or ethical consent must be distinguished from the legal basis used for the research.

4.2.1 General conditions for consent

Consent may be given in writing, electronically or orally. If, as a researcher, you use consent for data processing you must ensure that the individual's consent is:

- freely-given;
- specific to the research purpose(s) which must be highlighted to data subjects;
- informed; and
- unambiguous indication given by clear affirmative statement or action and clearly distinguished from other terms and conditions. Silence, pre-ticked boxes or inactivity cannot be used to give consent.

Researchers must allow data subjects to give separate consent for all personal data processing activities. Separate consents must always be sought to conduct research, re-contact data subjects for specified future research purposes and/or to use data subject video or visual images such as recordings and photos.

Written, electronic and oral consent are all valid but consent must always be verifiable in order to demonstrate that consent was legitimately obtained. For consent obtained orally this could include noting when and how consent was obtained against individual data subject records e.g. Jane Doe consented by phone on 25th May 2018 at 10:30 a.m. Note made by A. Researcher at 10:35 a.m. on 25th May 2018 together with a record of the script used in the conversation.

4.2.2 Conditions for explicit consent

Reliance on explicit consent is required for:

- collection of special category data or criminal offences or convictions data;
- automated decision-making and/or profiling with legal or significant effects; or
- international data transfers to countries outside the European Economic Area (EEA) that are not deemed adequate by the EU.[7]

[7] Countries within the EEA includes all EU countries and non-EU countries Iceland, Liechtenstein and Norway. The European Commission has so far recognised Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, Uruguay and the US (limited to the Privacy Shield framework) as providing adequate protection. Adequacy talks are ongoing with South Korea.

Explicit consent must be given by a very clear and specific statement of consent. EU guidance specifies that explicit consent can be obtained by a signed written statement; by the individual sending an email, uploading a scanned document carrying the signature or by using an electronic signature.

Researchers collecting special category data or criminal convictions data as a core part of a research project must ensure that they obtain and record a specific statement such as "Name/Signature/Data agree to take part in this research study which will collect data about my physical health and religious beliefs and attitudes."

Special category data and/or criminal convictions data may also be collected as part of a demographic classification exercise for research projects or as a requirement for equal opportunities monitoring. If answering these questions are optional (such as with a prefer not to say option) then explicit consent can be sought at the point that the classification questions are posed. Participants must be able to provide information in a way that reflects the view that they want to express and must not suffer any detriment as a result of failing to participate in a research project. If the special category data is being sought as part of equal opportunities monitoring, then these is a specific substantial public interest legal ground under DPA 2018 that can also be used.

If there is automated decision making and/or profiling of the data subject, then the data subject must be given information about the processing explaining what information will be used, why it will be used and what the effects might be. Also, if explicit consent is being used to authorise data transfers to third countries (in the absence of an adequacy decision and appropriate safeguards), then data subjects must be informed about the possible risks of these transfers.

4.2.3. Consent of children

Researchers must note that under the MRS Code of Conduct, children are data subjects who are under the age of 16. The Code requires that researchers seek the consent of a responsible adult prior to seeking the consent of a child (data subject under the age of 16) to participate in a research exercise. The standard of consent under the Code must be interpreted in line with the GDPR. This rule requiring adult consent for research with children applies to all channels of research e.g. online; digital; face-to-face; telephone or postal.

The age requirement in the Code is stricter than the requirements under the DPA 2018. Under the DPA 2018 the following rules apply:

- parental consent must be sought in relation to processing of personal data for online services, for children under the age of 13
- children over the age of 13 can give their own consent in relation to processing of personal data for online services
- competence of the child must be assessed where relying on consent and/or performance of a contract as the legal ground.

In all cases research exercises with children must be carefully reviewed to ensure children are properly protected when you are collecting and processing their personal data (particularly as they may be less aware of the risks). Additionally, privacy information notices must be tailored and written in a manner that is easily understood by the target age group of children or young people.

Researchers must always adhere to the MRS definition of a child as under 16, not to the age requirement for parental consent under the DPA 2018 for data subjects under the age of 13.

4.2.4. Recording consent

Robust records must be kept of all consents obtained demonstrating who consented, when they consented, what they were told, how they consented, whether they have withdrawn consent and if so, when. This should include:

- who consented (name of individual, or other identifier (e.g. online user name, session ID);
- when they consented (copy of dated document; online record with timestamp; note of time and date which was made at time of conversation);
- what they were told (master copy of document or data capture form containing consent statement used at time; record of scripts used in getting oral consent);
- how they consented (relevant document or data capture form; for online consent data submitted as well as timestamp to link to relevant version of data capture form; note of oral conversation but not necessarily a full record of conversation; audio recording of confirmation of the consent);
- whether they have withdrawn consent and, if so, when.

4.2.5 Minimum information requirements for consent

Data subjects must be provided with all relevant information to make choices about the collection and retention of their data. Different techniques and formats can be used to get consent for data collection but, in all cases, the consent must be specific and informed with transparent disclosure of all required information. Pre-ticked boxes or opt-outs are not allowed.

There is a minimum level of information that must be provided as part of the process of getting consent. As applicable this includes:

- data controller(s) identity and contact details –details of the data controllers relying on the consent (this may be both the research supplier/s and the client where they act as joint controllers) preferably allowing for different channels of communication (e.g. phone, email, postal address);
- purpose of each processing activity that consent is being sought for (such as for research, re-contact for future research);
- type of personal data to be collected and used;
- existence of the right to withdraw consent;
- information about the use of the personal data for decisions based solely on automated processing, including profiling; and
- possible risks of data transfers to third countries outside the EEA in the absence of an adequacy decision or appropriate safeguards.

This information must be provided prior to getting consent and must be included on a consent form or in the script being read to data subjects to seek verbal consent for their participation.

4.2.6. Data subject rights

In addition to the information that is provided to research data subjects as part of the process of obtaining informed consent, data subjects also have the right to the following specified information when consent is used as the basis for data processing:

- contact details of data protection officer(s) (if applicable);

- legal basis for processing;
- details of any international data transfer outside of the EEA;
- retention period for data or criteria for retention;
- existence of any automated decision making and logic, significance and consequences; and
- details of all other rights including right to object, right to data portability, right to withdraw consent; right to lodge complaints with supervisory authorities.

Data subjects also have other rights:

- to withdraw consent at any time (must be as easy to take away as to give);
- to port data (if automated information collection);
- to erasure of data made public (and data controller will need to inform other controllers who may be processing);
- to restrict processing;
- to access data;
- to rectify data held;
- to object to the processing; and
- to not be subject to decision based on automated processing (including profiling) which produces legal effects or significantly affects them.

All of the rights must be promoted at each contact point. If data subjects withdraw their consent for use of their data, the data controller must ensure that any personal data is deleted from any study or database in which the data subject is still identifiable.

If there are joint data controllers the privacy information notice that will be applicable to the research must be agreed between the controllers so that it can easily be made available to research data subjects. It must be completely clear to the data subject which data controller can be approached in order for them to exercise their rights under the GDPR.

In determining whether consent or another ground is the right ground. Organisations should note that consent can be withdrawn (and processing must stop immediately) however if an individual objects on the basis of legitimate interests an organisation has an opportunity to defend the decision. Additionally, an individual's right to erasure is automatic if processing is based on consent but it is not automatic for processing based on legitimate interests. In the later case of legitimate interest processing an individual has a right to object and the right to erasure would apply if the processing is not justified and if the data is no longer required for processing purposes.

All of this information must be set out in clear and plain language in a privacy information notice.

4.2.7 Consent for recordings and in digital environments

Consent for audio, video and other visual images

In seeking consent for the use of visual images, particularly video clips, researchers must ensure that:

- unambiguous consent is obtained in line with the standard of consent for personal data;
- data subjects have been fully briefed and informed about their use particularly where the video clips and/or images will be shared on social media platforms; and
- clients have agreed to use the visual images data only in line with the consents provided by data subjects.

Consent for electronic communications

- Collection of personal data in electronic communication services e.g. online services, will be impacted by the reforms to the e-Privacy Directive and Privacy Electronic and Communications Regulations in the proposed e-Privacy Regulation. This may lead to consent being used as the legal ground in additional situations, such as third party analytics used to measure and assess number of visitors to a website. Final version of the e-Privacy Regulation is expected in 2019.

Consent in practice

Consent is suitable for a range research approaches such as:

- Panel research
- Qualitative and quantitative research based on free found recruitment or recruitment of data subjects face to face, in store, in street recruitment or random digit dialling
- Customer satisfaction research
- Online or digital surveys

Consent Example: Qualitative study

A fieldwork agency is commissioned by a research agency to recruit members of the public to participate in focus groups assessing a brand's dental products. The research agency designs the screener and recruitment script. It also carries out the interviews (moderating the focus groups), analyses the data and writes the report for the client. At recruitment the data subject is provided with a consent form that allows them to sign and give a written declaration of their consent. The form details the name of the client and the research agency. It also sets out the purpose(s) of the research for which consent is being sought as to "gather views of the public on the packaging design of dental products". It allows the individual to consent separately to video recording and to re-contact for follow-up research on the same products by the client within the next 6 months. The consent form also sets out that the individual has a right to withdraw consent at any time. A full privacy information notice is provided at the time that the data subject signs the consent form.

In this case the research agency and the client will be joint data controllers, with the fieldwork agency acting as a data processor. This approach would be sufficient to get informed consent for the project. If the data subjects are being recruited on the basis of health characteristics e.g. regularly bleeding gums and/or the research will cover impact of the use of the products on their health, then it will be important to highlight that the research is health related (i.e. is special category data) in the consent statement to be signed by the data subject.

Additionally, to meet other data protection requirements, the agreement between the joint data controllers must also set out whose privacy information notice will be used and who the data subject should contact to exercise any of their data protection rights. The agreement between the research agency and the fieldwork agency should ensure that any personal data is securely transferred between them. Appropriate organisational and technical measures must be in place which will depend on the risk attached to the data and to the transfer.

Consent Example: Observation Research

Researcher displays a prominent notice in a supermarket informing data subjects that photographs and/or recordings are being made and used for research purposes. Members of the public having been so informed, decide to go to the area in which this is being done. Consent cannot be inferred by affirmative action in entering the building and an alternative legal processing ground will be required.

Consent Example: Telephone Survey

Research call centre carrying out a Random Dialled (RDD) survey asks data subjects for specific permission at the outset of a call for the survey research. Records of consent are kept in a spreadsheet with "consent provided" ticked against the data subject's name.

The oral consent is acceptable however it will need to be fully documented. Agencies need to keep details such as date, time, individual making call, script used. It may be best practice to have consent in a durable medium such as a recording that can be evidence of consent. Recording would start after consent obtained and confirm that interview proceeding as consent was given. Details of how data subjects can access the privacy information notice will also need to be provided such as by providing website link; offering to email data subject or providing a phone number they can contact to hear additional information.

Consent Example: Quantitative Tracking Study

Data subjects are required to click on a box to enter a survey. A privacy information notice is provided. A statement with a tick box signifying the individual's agreement is necessary for the collection of any special category data. Best practice requires that specific explicit consent is sought upfront for surveys where the main subject matter of the survey is on special category data. However, consent for collection of special category data such as for categorisation purposes can be sought at the point in the online survey where these demographic questions are asked of the data subjects.

For further information see:

- MRS GDPR In Brief (No.5): Informed Consent (Member Content)
- MRS GDPR In Brief (No.6): Informed Consent Checklist (Member Content)
- ICO Guide to the GDPR (consent) https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/

4.3 Legitimate Interest

Legitimate interest (LI) is a flexible processing ground that can be used as a basis for collecting and processing personal data in research projects. LI is likely to be most appropriate where the data is being used in ways that individuals would reasonably expect and the processing is unlikely to have a significant impact on their privacy.

In using LI organisations are processing data based on legitimate interests pursued by the data controller (such as a client) or on the legitimate interests of a third party. The type of interests that can qualify as legitimate interests are broad and include processing for all types of research purposes, as well as commercial activities such as direct marketing. However care must be taken with electronic direct marketing to ensure that requirements of the Privacy and Electronic Communication Regulations (PECR) are complied with. In determining whether LI can be used, organisations will need to ensure that their interests are not overridden by the fundamental rights and freedoms of the data subject. Particular care must be taken in considering the rights of children.

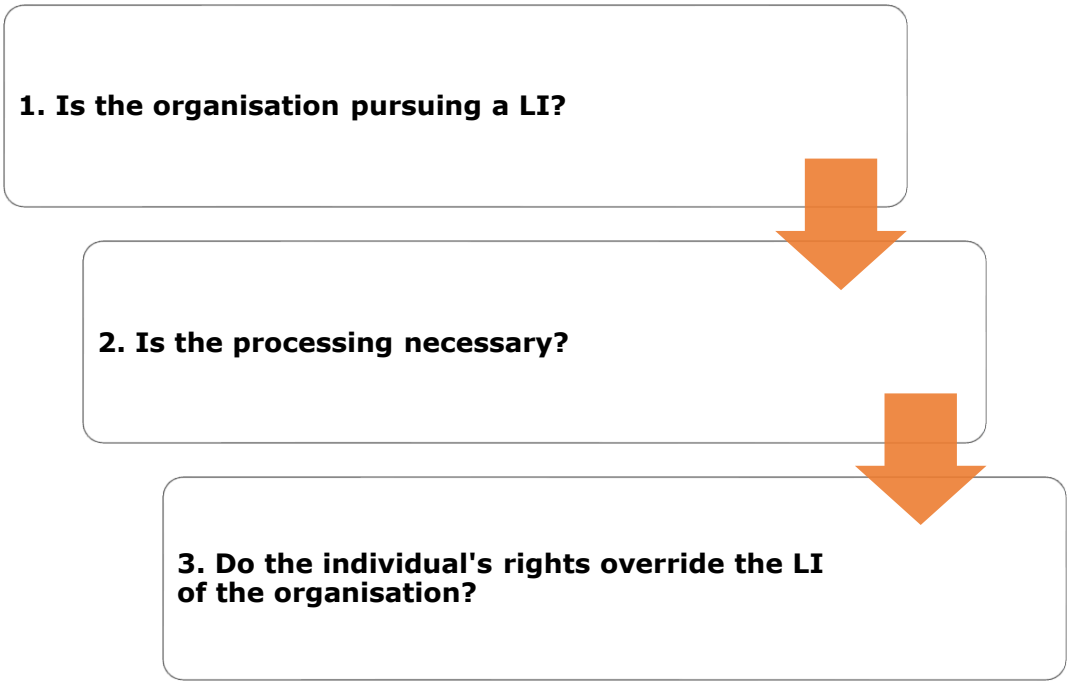
A range of interests will qualify as legitimate interests. It is important to be clear as to whose legitimate interests are being considered. The legitimate interests may be those of the researcher acting as a data controller, such as where a research agency recalls data subjects for quality control purposes, (even where they have not consented to a recall for research). They may also be the legitimate interests of the client as data controller, such as when a researcher contacts customers on a client database to ask them to participate in research to understand customer satisfaction levels with the client's products and/or service. It may also be a researcher's interest as a third party to access a database. The GDPR does not allow public authorities to use LI as a processing ground. However, under the DPA 2018, public sector bodies are likely to be able to rely on legitimate interest grounds when carrying out non-public tasks.

4.3.1 Legitimate Interest Assessment - Approach to using LI as a processing ground

Researchers using this processing ground will need to follow and document a three stage approach. The process of considering, weighing interests and making a justified decision must be applied and documented in a Legitimate Interests Assessment (LIA):

1. Purpose – Is a legitimate interest being pursued?
2. Necessity – Is the processing necessary?
3. Balancing – Do the individual's interests override the legitimate interest of the organisation?

Figure 4: The Legitimate Interest (LI) Test



Purpose Is there, and if so, what is the legitimate interest being pursued?

The GDPR sets out a non-exhaustive list of potential legitimate interests, including prevention of fraud. Regulatory guidance in this area also makes it clear that the nature of the interest can vary and encompasses trivial as well as compelling interests.

In order to identify the legitimate interest ICO recommends that organisations consider:

- Why do you want to process the data – what are you trying to achieve?
- Who benefits from the processing? In what way?
- Are there any wider public benefits to the processing?
- How important are those benefits?
- What would the impact be if you couldn't go ahead?
- Would your use of the data be unethical or unlawful in any way?

Necessity Is the processing necessary?

In order to use LI the processing must be necessary to pursue the interest. The proposed processing of the data does not have to be the only way to pursue the interest, but it should be a reasonable way of proceeding. This requires the organisations to consider the targeting and proportionality of the processing.

Organisations need to consider whether there are less intrusive or more privacy enhancing means of processing the personal data for the organisation's legitimate interests. The type of data being processed and context in which it was collected will all impact on the determination as to how intrusive the processing is.

In order to apply the necessity test the ICO recommends that organisations consider:

- Does this processing actually help to further that interest?
- Is it a reasonable way to go about it?
- Is there another less intrusive way to achieve the same result?

Balancing Do the individual's rights override the LI of the organisation?

The legitimate interests of the organisation must be balanced with the interests of individual. In order to balance interests by considering the impact of the processing and whether this overrides the interest the ICO recommends that organisations consider:

- What is the nature of your relationship with the individual?
- Is any of the data particularly sensitive or private?
- Would people expect you to use their data in this way?
- Are you happy to explain it to them?
- Are some people likely to object or find it intrusive?
- What is the possible impact on the individual?
- How big an impact might it have on them?
- Are you processing children's data?
- Are any of the data subjects vulnerable in any other way?
- Can you adopt any safeguards to minimise the impact?
- Can you offer an opt-out?

It is important to look at the

- impact on data subjects such as the possible level of harm;
- way the data is being processed;
- reasonable expectations of data subjects; and
- safeguards that could be put in place.

Balancing the data controller's rights against the rights of the individual in a research context means that you should structure and carry out the research in the least intrusive and most privacy-enhancing way.

Organisations need to keep a written record of reasons why it is felt the balancing test was met. This important in order to meet the GDPR accountability principle.

Conducting market, opinion and social research activities is likely to fall within the legitimate interests of the data controller, but as discussed, written documentation justifying this must be developed and kept by the data controller.

4.3.2. Limitations of LI

Although LI is a flexible processing ground it places an onus on the organisation attempting to use it to ensure that individual's rights and interests are fully considered and protected.

LI cannot be used as a processing ground:

- by public authorities (unless the processing is outside their scope of tasks as a public authority);
- for automated decisions based on profiling activities;
- for processing of special category data unless an additional condition under Article 6 is also used.

LI should be used with caution as a processing ground for children's personal data and extra care taken to ensure interests of children are fully protected. It is also important that researchers ensure that in line with the MRS Code of Conduct personal data of children under 16 is only collected after seeking consent of a responsible adult to approach the child to get their consent.

4.3.3. Transparency and LI

In order to rely on LI the organisation must set out its legitimate interests in privacy information notice. Researchers relying on LI to carry out research on customers databases for example would need to ensure that a proper explanation of LI for research has been included in the client's privacy notice setting out the basis for using LI.

Example of LI statement

Name of organisation/We process personal data/information for certain legitimate business purpose which include undertaking research to:-

- *better understand how people interact with our websites*
- *better understand how people choose and/or use our products and services*
- *determine the effectiveness of our promotional campaigns and advertising*

Data subjects have similar rights to situations where processing is based on consent, but they also have the right to object to processing for legitimate interests without providing specific reasons. Also, data subjects do not have a right to port or move their data (as this only applies where data gathered on the basis of consent or contract) and the right to erasure is not automatic as it is with processing based on consent.

Legitimate interests in practice

Legitimate interest is suitable for a range of approaches including:

- Customer satisfaction, awareness and usage surveys (on customer databases)
- Quantitative or qualitative research using customer databases
- Research using existing data sets or third party data (i.e. data not directly provided by individual or where no contractual relationship) such as social media analytics
- Secondary processing such as data analytics on loyalty card data or on mixed brand datasets customer behaviours, preferences and movements. If unable to contact all participants then need to use the flexibility in the information obligations where contacting all participants for scientific research would involve a disproportionate effort

Legitimate Interest: Client supplied list

Client company transfers customer data list to a research company for the supplier to develop a sample/target group for satisfaction research exercise. List includes customers who have objected to being contacted for marketing. The list can be used on the legal basis of legitimate interests of the client once the LIA has been undertaken and the client's interest is compatible, the client's privacy note details their legitimate interests as including research and no special category data is being collected as part of this exercise. Researcher must check that the opt-out from marketing contacts is not drafted so widely as to cover opt outs from market research.

Decision making process for this must be documented.

Legitimate Interest: Audience measurement

Radio station commissions a research agency specialising in audience measurement to provide data on audience/ visitors. The analytics are used to assess number of visitors, page views etc. for tailoring/optimisation of future marketing campaigns. Aggregate reports are provided grouped under headings such as age brackets, gender, geographical location, socio-economic bands). Aggregate reports are produced for the client. Agency pseudonymises data and disposes of data after original purpose fulfilled. Contract between the client and research agency prohibit attempts to re-identify data. Reports are not used for individual targeting or advertising to research data subjects.

This may be an allowable legitimate interest under GDPR. It is an area where the legal requirements may become more stringent following the proposed ePrivacy Regulation and reform of Privacy and Electronic Communication Regulations (PECR). Balancing test will need to be carried out and documented detailing the business interests and individual's right.

For further information see:

- ICO Guide to the GDPR (Legitimate Interests) https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/
- DPN Guidance on the use of Legitimate Interests under the EU General Data Protection Regulation (July 2017) https://www.dpnetwork.org.uk/dpn-legitimate-interests-guidance/
- IAF Legitimate Interests and Integrated Risk and Benefits Assessment (September 2017) http://informationaccountability.org/wp-content/uploads/Legitimate-Interests-and-Integrated-Risk-and-Benefits-Assessment.pdf

4.4 Contract

Contract can be used as a legal basis for processing personal data. Researchers can rely on this if they need to process someone's personal data in order to fulfil their contractual obligations to them. This ground will be of limited use but may be applicable to administration and management of research panels.

Panel providers can use contracts as the legal basis for recruitment to research panels for processing that is necessary for the contract between them and the research panellist. Data subjects are likely to join a panel on the basis of the terms and conditions of the research panel provider. These terms and conditions together with the privacy policies and notices will provide information to data subjects about the collection, processing, use and storage of aggregated and personal data, plus any specifics relating to the providers activities.

If contractual necessity is being used as the legal ground this must be documented, with reasons clearly set out in the organisation's records. Data subjects must also be informed that this is the basis for processing their personal data. This ground is likely to be applicable only to the arrangements for adding a panellist to the panel database. Collection of personal data for individual research projects e.g., surveys will need to be conducted on the basis of consent and in particular contract cannot be used a ground for processing special category data. This will generally be processed on the basis of explicit consent of the data subject.

A contact does not have to be in writing in order to be legally binding however researchers using this ground must ensure that the terms and conditions with panellists are recorded in writing so that they have a full documented record of what has been agreed between the parties.

For processing based on contractual necessity, data subject rights are applicable including their right to port data but

- no right to object to processing; and
- no right not to be subject to a decision based solely on automated processing (if the automated decision is necessary for entry into or performance of the contract).

Contract in practice

Contract is not generally a suitable basis for processing research data but can be used in the following circumstances:

- General terms and conditions for administration of the panel
- Incentives payment and management

4.5 Further processing (Secondary use of personal data)

In line with the purpose limitation principle in the GDPR, personal data must be collected for well-defined purposes and not further processed for additional purposes. Exceptions to this are where the secondary use of the data is:

- based on consent;
- compatible with original data collection purposes;
- for scientific or statistical research purposes; or
- based on an EU or Member State law.

Secondary use of data occurs when data is used for a purpose different from the purpose for which the data was initially collected. A processing ground is still required for this secondary use of data and the GDPR sets out a compatibility test for re-use of data not based on consent.[8] Transparency of processing is also important for secondary use of personal data and information requirements (for processing of data not directly collected from the data subject) must be adhered to.

4.5.1 Further processing based on consent

Personal data can be further processed if consent for the specific purpose has been obtained from the individual at the outset of data collection. If the data controller processes data based on consent and wishes to process the data for a new purpose, then the controller needs to seek a new consent. There is no scope for processing for further "compatible" purposes to inherit the original consent as a basis for processing. In light of this, researchers must define as well as possible any further, secondary purposes when collecting consent at the outset of the research project. If the research project is scientific research in the public interest it may be possible to provide additional information with greater granularity as the project progresses but this should not be used as a default option. Additional information on using the research regime is set out in section 5 of this Guidance.

4.5.2 Further processing based on legitimate interests

Legitimate interests of the data controller can also be used to further process data as long as this processing is for a compatible purpose.

Key points in determining compatibility are (this is not a limited list):

- Link between the purpose the personal data was initially collected for and the purpose it is proposed the data be used for
- Context and relationship between the data subject and the data controller
- Nature of the personal data
- Possible consequences of processing the personal data
- Safeguards used in processing such as encryption or pseudonymisation of data

Researchers will generally be able to justify the further use personal data (initially collected for another non-research purpose) using the legitimate interests of the data controllers/clients as the processing ground. In these circumstances, a research purpose is likely to be compatible with the original data collection and processing purpose.

[8] GDPR Article 6(4)

If personal data is being used for scientific and/or statistical research it is deemed compatible under the GDPR.

Researchers must first check to see whether a research project can be carried out with de-identified or anonymised data. It is also important to recognise that special category data can only be re-used where explicit consent is provided. Remember that special category data cannot be processed on the basis of legitimate interests unless there is an additional processing condition.

Further processing in practice

Further processing can be used for a range of research approaches such as:

- Re-using data for research
- Purchased secondary data
- Sharing purchased data
- Open access secondary data

Further processing: Data analytics

Retailer using loyalty card data gathered for research. Reasonable expectation that retailer would use this data to gain a better understanding of customers and the market. Acceptable and likely compatible further processing using legitimate interests as the legal processing ground.

Further processing: Combining datasets

Retailer looking across datasets and combining this with other publicly accessible data (such as information legally obtained (i.e. in accordance with the terms and conditions) from social media platforms Facebook, Twitter, Pinterest, LinkedIn) to instruct interaction with particular data subjects (e.g. targeted advertising). It is unlikely this would meet the compatibility requirements for further processing based on legitimate interest. It would also require analysis of other rules such as direct marketing/profiling and requirement to ensure compliance with data minimisation principle and conduct a DPIA.

For further information see:

- *ICO Guide to the GDPR*
  https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/

4.6 Summary

Table 3 Research processing grounds and conditions

Processing Ground/Condition	Category of Data	Types of Research Activity	Public-facing documentation
Contract	Personal	Use for general terms and conditions for administration of the panel and incentives management for panellists rather than for research activity.	Contract terms and conditions Privacy policy
Consent	Personal Special Category Criminal Convictions	Panel research Qualitative and quantitative research (free found recruitment or recruitment of data subjects face to face, in store, in street recruitment or random digit dialling) Customer satisfaction research Online or digital surveys Further processing based on new consent	Consent statement Privacy Policy Special category policy document (as applicable)
Legitimate Interests	Personal	Customer satisfaction research (on existing customer databases) Quantitative or qualitative research using customer databases Research using existing datasets or third party data (i.e. data not directly provided by individual or where no contractual relationship) such as social media analytics Data analytics on loyalty card data Compatible further processing of data collected using another processing ground	Summary of Legitimate Interest Assessment (make available) Privacy Policy setting out legitimate interests
Scientific research purposes in the public interest *	Special Category Criminal Convictions	Published social research projects Public health research Longitudinal studies	Special category policy documentation Summary of public interest assessment (make available)

*See further discussion of public interest in Section 5 of the Guidance

Section 5:
Public Interest Research

This section discusses research by or for public bodies and the research regime that is applicable to scientific research in the public interest under the DPA 2018.

5.1 Public sector bodies

Although the majority of provisions in the GDPR apply to all data controllers or data processors, there are some requirements that will apply differently to public sector bodies ("public authorities"). This includes limits on the processing grounds that can be used and the mandatory requirement to appoint a data protection officer.

5.1.1 Definition of public authority/public body

A public authority under the DPA 2018 is as defined by the Freedom of Information Act 2000, the Freedom of Information Act (Scotland) 2002 and any authority or body specified by the Secretary of State in Regulations. This currently includes broad categories including Government departments, legislative bodies, and the armed forces; local government; National Health Service; maintained state schools and further and higher education institutions such as universities; police; and other named public bodies.

5.1.2 Processing grounds and conditions for public authorities

Processing grounds that are likely to be used by public authorities processing personal data under the GDPR and DPA 2018 are set out in Figure 5. These include:

- unambiguous consent (as long as there is not an imbalance of power between the public authority and the data subject)
- performance of a task carried out in the public interest or in the exercise of official authority vested in the controller "public task"[9]
- compliance with a legal obligation

Additionally, the processing conditions most likely to be used for special category data are:

- explicit consent
- substantial public interest
- scientific research in the public interest

[9] Article 6(3) and Recital 45 make clear this ground will apply only where the task carried out, or the authority of the controller, is laid down in Union law or Member State law to which the controller is subject. This ground can only be used if carrying out official functions.

In a divergence from the GDPR, public sector bodies in the UK can rely on legitimate interests when carrying out non-public tasks. An organisation will only be a public authority "when performing a task carried out in the public interest or in the exercise of official authority vested in it." For example, the non-core functions of a university are likely to be alumni relations and fundraising for which legitimate interests can be used as a base as appropriate.

Data sharing gateways such as those set out in the Digital Economy Act 2017 may also provide important avenues for data processing in specific circumstances.

5.2 Public interest

Public interest considerations will be of particular importance in the following situations:

- *Using public task as a processing ground* **-** Public task provides a basis for processing where laid down in law. This will include public authorities with research as an incorporated or statutory purpose (including NHS organisations and universities which can use their University Charter). If using "public task" as a legal basis this must be internally documented and justified by reference to the statutory public research purpose.
- *Using scientific research in the public interest as a processing condition* **–** Public authorities can also collect special category data when conducting scientific and/or statistical research in the public interest.

The GDPR and DPA 2018 do not set out a specific public interest test as this is likely to vary between sectors. It is important that any public interest test considers how best to balance public interest with fundamental rights and freedoms of individual in conducting market and social research.

It is clear that the public interest can cover research of wide benefit to society and the economy and covers research carried out by both commercial and non-commercial researchers, such as those based in university research centres, think-tanks, charities, not-for-profit and commercial research organisations.[10]

Researchers will need to carry out a balancing test, assessing the public interest in light of individual rights and freedoms. The approach to this will be similar to that used in assessing a legitimate interest.

Issues to consider include:-

- What is the public interest being pursued?
- Is the processing necessary for the public interest?
- Do the data subject's rights override the public interest being pursued?

[10] See further MRS SRA Data Protection Guidance (Forthcoming Summer 2019)

Figure 5: Public authorities processing grounds (Articles 6,9, 10 GDPR; Sections 8, 10; Sched. 1 DPA 2018)

5.3 Research exemption

The GDPR and DPA 2018 contain a specific legal framework for personal data processed solely for specified research purposes. These special rules have been developed for research in recognition of the importance of a strong science base and the fact that the use of personal data is critical in providing insights and ensuring quality and reliability in scientific research. They are intended to support the objective of achieving a European Research Area to support innovation and advancements in medicine, science and technology and ensure the EU remains competitive in world markets.

The "research exemption" applies to archival, scientific, statistical and historical research purposes. The exemption is applied on a case by case basis and the applicability/necessity of use of the exemption must be a preliminary consideration. It provides greater flexibility for necessary processing for research purposes particularly around certain data subject rights and notice requirements. It can be used by all researchers (whether based in private sector, public sector, charity sector or academia) depending on the type of research that is being conducted. Although this framework affords researchers with a certain level of flexibility, it should be noted that most of the provisions of the GDPR/DPA 2018 will still apply.

5.3.1 General conditions for the research exemption

The research exemption is set out in section 18 of the DPA 2018 which implements Article 89(1) of the GDPR.

Controllers processing personal data for scientific research purposes can take advantage of the following exemptions and exceptions from the GDPR provisions:

Exemptions and exceptions from certain rights

The following rights do not apply:

- right of the data subject to object to processing of personal data (where necessary in the public interest)
- right to restrict processing pending verification or correction
- right to have inaccurate data rectified

The GDPR also provides for exceptions from provisions on the right to be informed and the right to erasure:

- Right of data subjects to exercise their "right to erasure" is restricted if it is likely to significantly impair processing for scientific research purposes
- Limitations are placed on the right of data subjects to be informed (for indirectly collected data)

The DPA 2018 does not use the additional GDPR flexibility on the right of a child to be forgotten and researchers must fulfil these rights when requested by a data subject.

Adaptations to data protection principles

Additionally the GDPR also limits the application of the purpose limitation and storage limitation principles so that researchers conducting scientific research have the:

- ability to use personal data collected for other purposes for research purposes
- store personal data for longer periods
- make isolated transfers of personal data to countries outside the European Economic Area (EEA) taking into account legitimate expectations of society for an increase in knowledge; and
- limit obligations on level of information provided to data subjects in scientific research if it would involve a disproportionate effort.

5.3.2 Safeguards

Use of the research exemptions and exceptions is not automatic. Controllers seeking to use the research regime must consider:

- necessity of the processing;
- extent to which compliance with standard data protection requirements would impair the processing purposes;

and meet the conditions and safeguards as discussed below.

Appropriate safeguards to protect the right and freedoms of data subjects

Under the DPA 2018 it is specified that the processing of the data must be exclusively for research purposes, and, the appropriate safeguards that need to be met include:

- not for measures or decisions with respect to the particular data subjects (unless necessary for approved medical research); and
- no likelihood of substantial damage or substantial distress to any data subjects.

and as regards the right of access, the research results are not made available in a way that identifies individuals.

Adequate technical and security measures

Technical and organisational measures must also be in place such as:

- Data minimisation by only collecting information that is necessary such as by minimising the number of participants, data per participant or degree of sensitivity;
- Use of pseudonymised data by default; and
- Access controls that ensure that only those who need to know are allowed access to personal data.

5.3.3 Consent for scientific research

In seeking consent for scientific research purposes, under the research exemption, all the standard general conditions for consent are expected to be met. However, in limited circumstances if the research purposes cannot be fully specified at the outset, then the data controller(s) should use transparent mechanisms to meet the essence of the consent requirements. This could include seeking consent in stages before each phase of the research begins and supplying participants with a comprehensive research plan at the outset of the research. Rigorous safeguards such as data minimisation, anonymisation or data security must always be applied, as with any research exercise. Standards set out in the MRS Code of Conduct must also be followed.

5.3.4. Transparency and research exemption

Article 14 of the GDPR provides for exceptions to the requirement to provide information in circumstances where the personal data has not been obtained directly from the data subject. This includes where:-

- it proves impossible (in particular for archiving, scientific/historical research or statistical purposes)
- it would involve a disproportionate effort (in (in particular for archiving, scientific/historical research or statistical purposes)

Points to take into account in determining this include the number of data subjects, the age of the data and any appropriate safeguards adopted. Appropriate safeguards must be taken, as is the case in all processing using the research exemption.

Research exemption in practice

Research exemption is suitable for a range of approaches including:

- Published social research projects
- Public health research
- Longitudinal studies

Public Interest: Dementia research

Research conducted on behalf of a charity in order to produce a rich and detailed understanding of the day to day lives of both people living with dementia and their carers, and to identify how people would like to be supported. Findings inform and support the charity's strategy and public advocacy. Research likely to be considered in the public interest as provide an evidence base for decisions likely to benefit the society and quality of life of people in the UK. Research exemption could be used as a basis to keep personal data for a longer period (subject to appropriate safeguards) if for example wished to repeat the survey and compare findings over a ten-year period.

Public Interest: Product instructions

Research conducted on instructions for non-prescription health product to ensure legible and easily understood by customers. If public interest is construed broadly this could fall within the public interest ensuring appropriate use of products by individuals.

Public Interest: Product branding design

Research conducted on branding of competitive non-prescription health product to determine which type of packaging considered more attractive by customers. This is unlikely to meet a public interest test as is purely research to obtain a competitive advantage.

codeline@mrs.org.uk

Codeline offers email support and advice on the MRS Code of Conduct, Regulations and Guidelines. Data protection guidance is provided as general information for research practitioners. It is not legal advice and cannot be relied upon as such. Specific legal advice should be taken in relation to any specific legal problems or matters.