Principles of the General Data Protection Regulation (GDPR) & Data Protection in a Research Context:

A Guideline for Researchers

Key Facts

The European Union's (EU) General Data Protection Regulation (GDPR) was enacted on the 25th May 2018, replacing the now superseded EU Data Protection Directive.

The GDPR is directly applicable at national level and harmonizes data protection laws across the EU. It replaces the 1995 Data Protection Directive (Directive 95/46/EC).

The GDPR covers EU residents' personal data, including data processed for clinical trials, registries and medical research projects and applies directly to companies located within the European Economic Area (EEA). It applies to data controllers and data processors established in the EU and also to organisations located anywhere in the world who are processing the personal data of EU residents, where such organisations are:

a) Offering goods or services in the EU, or (i.e., partnering on a research project with a European collaborator)
b) Monitoring of behaviour of participants within in the EU, as far as their behaviour takes place in the EU.

Note: If you are unsure whether the GDPR applies to your particular study or scenario, we suggest researchers consult with the Melbourne Children's Trial Centre (MCTC) MCTC@mcri.edu.au and MCRI Legal Office (legal@mcri.edu.au) for guidance.

Introduction

Research projects undertaken in Europe by the Murdoch Children's Research Institute (MCRI) or its collaborators often involve the collection of personal/health information. This information must be processed in accordance with the requirements of relevant data protection laws.

The purpose of this guideline is to introduce researchers to the provisions of the following legislation on data protection:

The European General Data Protection Regulation (GDPR) – EU Regulation No. 679/2016)

The introduction of the European Union (EU) General Data Protection Regulation (GDPR) is the most important change in data privacy regulation in 20 years. The aim of the GDPR is to standardise and strengthen the protection of EU residents' personal data across the EU and internationally.

As such, the GDPR has extra-territorial scope, meaning the GDPR applies to the processing activities of organisations that do not have a presence in the EU, but are processing the personal data of participants residing within the EU. **Therefore, an organisation that is not established within the EU (i.e., MCRI) will still be subject to the GDPR when it processes personal data of participants who are residents within the EU.**

There are significant financial penalties for contraventions of the GDPR .

The implications of the GDPR for research will be explained with particular reference to the following questions and issues:

1. What is data protection?
2. Why is data protection important?
3. Does your project involve information to which the GDPR applies?
4. What is special category personal data?
5. Who is responsible for complying with the GDPR?
6. What are your duties and obligations under the GDPR?
7. Can personal data be transferred to a country or territory outside the European Economic Area (EEA)?
8. Are there any relevant exemptions?
9. Practical considerations

A note regarding Brexit – UK Considerations

The GDPR entered into force in the United Kingdom (UK) on 25 May 2018, at which point the UK was a full Member State of the EU. The UK left the EU on 31 January 2020.

Whilst the UK formally ceased to be an EU Member State at that time, the EU – UK Withdrawal Treaty provides for a transition period lasting until the end of 2020 (unless extended by joint agreement). During the transition period, EU law (including the GDPR) continues to apply directly to the UK, and the UK will be treated as if it were a Member State for the purposes of that law. Following the end of the transition period, subject to the terms of any future trade agreement reached between the EU and the UK, EU law will cease to apply in the UK.

The UK Government will implement the GDPR into UK national law (creating the "UK GDPR"), subject to a number of technical changes (e.g., to amend references to "Member State" to the "United Kingdom") made under the Data Protection Act 2018, the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019.

Therefore, if your research includes participating/collaborating sites located within the UK, but no other countries within the EU, your research will still be subjected to GDPR regulations and MCRI must comply with these regulations.

Should researchers require further guidance around GDPR, particularly in applying legal requirements to specific projects, this is available from the Melbourne Children's Trial Centre (MCTC@mcri.edu.au) and the MCRI Legal Office (legal@mcri.edu.au).

1. What is Data Protection

In policy terms, data protection law aims to strike a balance between:

- The privacy interests of individuals; and,
- The needs of organisations to make fair and reasonable use of information relating to those individuals in their operations.

It does not mean that researchers cannot make use of such information, or that they must always have an individual's consent to do so, but it does impose controls and restrictions which must be complied with.

Technology has made it possible to collect and use increasing amounts of information about individuals in ever more diverse ways. The GDPR will introduce a new framework to safeguard the rights of those individuals.

2. Material Scope of the GDPR (Article 2)

The GDPR applies to the processing of personal data. Personal data is defined as any information relating to an identified or identifiable natural person and includes data such as an IP address, an email address or a telephone number. Processing activities include, among others, the collection, use and disclosure of the data.

The GDPR provides for additional protection to the processing of special categories of personal data. Such special categories include, personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership and genetic and biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

3. Why is Data Protection important?

MCRI is committed to responsible processing of information relating to individuals and to respecting their rights to data privacy.

If the GDPR applies to an organisation, and it fails to comply, this may have serious financial, reputational, and other consequences for the organisation. Breaches of data protection law may result in investigations, significant fines, adverse publicity, and civil or criminal liability. Enforcement action may be taken by various regulatory authority or bodies, for example, the UK's Information Commissioner's Office (the "ICO") has the power to issue fines or request changes in an organisation's policies and procedures prior to approval.

Should MCRI fail to comply with its legal obligations, such an action could be taken against MCRI and published on the ICO's website, resulting in reputational damage. Other implications refer to an individual's rights under GDPR. These may be exercised by submitting requests to MCRI in relation to the institute's use of their data (refer to Section 8 below for further information). If an individual is dissatisfied with the MCRI's response, they may complain to the relevant regulatory authority (such as the ICO). Individuals may also bring legal claims for privacy breaches.

4. Does your Research/Project involve information to which the GDPR applies?

The GDPR only applies where an organisation is involved in the "Processing" of "Personal Data" as those terms are defined in the GDPR. Guidance as to the meaning of "Processing" and "Personal Data" is set out below:

4.1 Are you a "Processor" of Data?

Processing is defined very broadly in the GDPR to mean almost anything a research team might do with personal data, including: collecting it; holding or storing it; retrieving, consulting, or using it; organising or adapting it; publishing, disclosing, or sharing it; and even destroying it.

4.2 Does your Research/Project involve Personal Data?

4.2.1 Personal Data

Personal data is information which relates to a living individual located in the EEA who can be identified from that information, whether directly or indirectly, and in particular by reference to an identifier. It includes, for example, a name, an identification number, location data, or an online identifier, such as the IP address, provided that information can be linked to a living individual. It could also include information that identifies an individual's characteristics, whether physical, physiological, genetic, cultural, or social.

This definition is intentionally broad, and its application to particular types of research data is considered in more detail below. Where there is any doubt as to whether your project is processing personal data within the scope of the GDPR, it is advised that you err on the side of caution and proceed on the basis that the GDPR does apply.

4.2.2 Pseudonymous Data

Under the GDPR, pseudonymous data is treated as Personal Data; furthermore, only anonymized data are excluded from the requirements of the GDPR. Pseudonymization of personal data refers to the act of altering personal data to the extent that the data subject cannot be directly identified without having further information, which is stored separately (Article 4(4) GDPR). This usually involves the removal of the usual direct identifiers and the use of a pseudonym (often a randomly allocated number), so that data can be continually collected about the same individual without recording their identity.

Pseudonymising data can be useful in research. Pseudonymous data can be collected in such a way that no re-identification is possible (e.g., one-way cryptography), in which case it is essentially anonymous data and the considerations above apply. However, it is often retraceable (e.g., key-coding, and two-way cryptography) and therefore, may continue to be Personal Data. Where the researcher (or any other person operating within the Institute) possesses the means to identify any of the individuals to whom the information relates, that information will still constitute Personal Data.

4.2.3 Anonymous Data

The GDPR does not contain a definition of what constitutes anonymous data. However, the fifth and sixth sentence of Recital 26 states that the *"principles of data protection should (…) not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes."*

Where that individual cannot be identified, and it is not possible to re-identify the individual, the information does not constitute Personal Data. As such, the duties, and obligations of the GDPR do not apply.

Researchers should, however, consider whether or not an individual is re-identifiable, notwithstanding the removal of the usual direct identifiers. Indeed, a combination of details on a categorical level (e.g., age, regional origin, medical condition, etc.) may allow an individual to be recognised by narrowing down the group to which they belong.

In determining whether an individual is re-identifiable, account should be taken of all the means reasonably likely to be used to identify that individual, whether by the research team or by any other person.

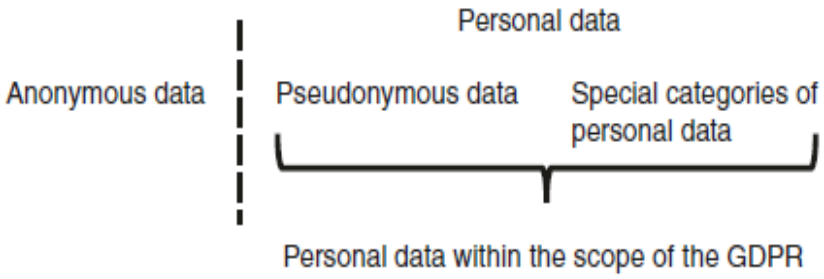


Figure 1: Categories of Personal Data under the GDPR

4.2.4 Aggregated Data

Aggregation is the process of combining information about many individuals into broad classes, groups, or categories, so that it is no longer possible to distinguish information relating to those individuals. It follows that this data should not be Personal Data, but its effectiveness will depend on such factors as the size of the population in which the individual is concealed.

4.2.5 Biometric Data, DNA and Human Tissue Samples

The definition of Personal Data in the GDPR includes biometric data and genetic data, where it allows the unique identification of an individual. The term biometric data is used to describe those intrinsic, biological, physical, or behavioural traits that are both unique to an individual and measurable. Examples commonly include fingerprints, retinal patterns, facial structure, voice, hand geometry, and vein patterns; but biometric data also includes deeply ingrained skills and behaviours (e.g., a handwritten signature and a particular way of walking or speaking).

Human tissue samples may provide a source from which Personal Data can be extracted, but they are not Personal Data themselves; that is, the extraction of information from samples may result in the collection of Personal Data. The collection, storage and use of tissue samples are subject to different laws, noting that those samples may be accompanied by information (e.g., name, age, etc.) which also constitute Personal Data.

4.2.6 Photographs, Videos and Sound Recordings

Where an individual participates in research which involves a recorded interview, that individual may disclose Personal Data about themselves or other people. However, researchers should also be aware that the existence of photographs, videos, and sound recordings of people (whether or not those individuals voluntarily disclose any information) may comprise information about that individual and may allow that individual to be identified. Accordingly, these are media which are capable of being personal data.

5. What is Special Category Personal Data?

The GDPR recognises that some categories of personal data are particularly private and/or could be used in a discriminatory way. As a result, the GDPR requires researchers to treat this "special category personal data" with greater care.

Special Category Personal Data includes any personal data consisting of the following information:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data for the purpose of uniquely identifying a person
- Health; and
- Sex life and sexuality.

Information about criminal convictions and offences is not included in the definition of special category personal data, however such information may be processed only under the control of official authority or when authorised by domestic law, which provides for appropriate safeguards.

Due consideration should be given to information which may indirectly disclose special category personal data about an individual. For example, photographs and names may give an indication of a person's race or religious beliefs however will not always be special category data merely because an assumption about a person's race or religious belief might be drawn from appearance or name. The issue will arise if that information is processed on the basis of those assumptions (for example, grouping people based on skin colour or likely ethnic origin of surname). The additional legal requirements in relation to special category personal data are described below (Refer to Section 6.0).

6. Data Protection and Consent

The health data collected in clinical trials, registries, and medical research projects — including biometric and genetic data — is sensitive personal data and the requirements of the GDPR will need to be considered for all planned or ongoing projects.

6.1 Consent

Where an organisation is relying on consent for the Processing of Personal Information, such consent must be explicit, unambiguous, and freely given. Note that this is required both by Good Clinical Practice (GCP) and the GDPR.

Combining the information required by the GDPR with the information required by GCP could result in very lengthy consent forms. Data Controllers (i.e., Sponsors) should consider ways to balance the amount of information given with the patient's ability to understand it, seeking to simplify the message whilst ensuring compliance with both sets of requirements.

All organisations involved in clinical trials, registries and medical research projects should maintain documented evidence of any consents obtained and of the steps taken to comply with the GDPR.

5.1.1 Withdrawal of Consent

A data subject has the right to withdraw their consent to the Processing of their Personal Information at any time. However, despite a withdrawal of consent, the GDPR allows organisations who are Processing Personal

Information for medical research to continue to store, use and otherwise process the Personal Information in certain circumstances (Refer to Section 9.0 below for further information on GDPR Exemptions).

However, data may only be kept if there is a legal basis for doing so (other than consent). Where there is no legal basis for justifying the further storage of such personal data after the withdrawal of consent, these data should be deleted/destroyed wherever they are stored.

7. Who is Responsible for complying with the GDPR?

The GDPR imposes obligations on both "**data controllers**" and "**data processors**".

A **"data controller"** is the person/institution/company who (either alone or collaboratively) holds the data and is responsible for its protection. Furthermore, a data controller makes decisions about processing activities. They exercise overall control of the personal data being processed, determines the purposes for which and the manner in which any personal data are, or are to be, processed and are ultimately in charge of and responsible for its processing.

The **"data processor"** is a person/institution/company who processes personal data on behalf of the data controller and is responsible for its correct and secure handling. Processors act on behalf of the relevant controller (e.g., under a contract of service).

For multi-centre, international research projects sponsored or initiated by MCRI, whereby you are recruiting, or enrolling participants based within the UK or EEA, MCRI will most likely be the **data controller.**

The GDPR requires data controllers, at the planning stage and at the time of processing, to take appropriate steps to meet the requirements of the GDPR and protect the rights of the data subjects. Data controllers must also be able to demonstrate their compliance with the GDPR (see 7.17 below).

Where the Institute is the data controller and you intend to supply any personal data to a third party to perform any subcontracted work (i.e., to act as the data processor), such transfer must be made under an appropriate contract which meets the requirements of the GDPR and includes specific clauses setting out the obligations of the data processor.

Where the Institute and a third party are jointly designing and collaborating on a research project, both the Institute and the third party are likely to be data controllers. In this situation, an agreement should be in place between the Institute and the third party setting out their respective responsibilities for compliance with the GDPR.

If MCRI is the data processor rather than the data controller in respect of processing of personal data (e.g., where work is being performed on behalf of another party who determines the means and purpose of processing for the Institute), the obligations of the GDPR will still apply to MCRI as a data processor. This would mean, for example, that MCRI would be responsible for ensuring the security of the data and for keeping records of any data processing activities. MCRI's obligations as data processor need to be set out in a contract with the data controller.

8. What are your Duties and Obligations under the GDPR?

8.1 Data Protection Principals

Researchers must process all personal data in accordance with the "**Data Protection Principles**" set out in Article 5 of the GDPR unless there is a relevant exemption (Refer to section 9.0 below for GDPR Exemptions).

As outlined in more detail below, under the Data Protection Principles personal data must:

- Be processed lawfully, fairly and in a transparent manner
- Be collected only for specified, explicit and legitimate purposes, and not be further processed in any manner incompatible with those
- Be adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed
- Be accurate and, where necessary, kept up-to-date
- Not be kept as identifiable data for longer than necessary for the purposes concerned; and
- Be processed securely.

8.1.1 Fair, Lawful and Transparent

a) Fair Processing

'Fair' processing requires researchers to consider more generally how their use of personal data affects the interests of the individuals to whom it relates. In circumstances where your use may cause detriment to an individual, you need to consider whether or not that detriment is justified. Fairness is naturally linked also to the transparency of the processing and the ability of the individual to object.

b) Lawful Processing: Personal Data

The processing of personal data must have a lawful basis (a legally acceptable reason for processing the data), which must be documented by the data controller. Of the six possible legal bases specified in the GDPR, three are of particular relevance to research and described further as follows:

Lawful Basis for Processing	**Description**

Consent	**This will likely be the most common legal basis for MCRI processing.** The consent of the individual to whom the information relates provides a lawful basis for the processing of personal data, whether that consent is obtained by MCRI directly from the individual concerned or indirectly by a third party contributor to the research project. Care needs to be taken over the form of any document seeking consent to ensure that consent is specific, informed, unambiguous and has been freely given for the purposes for which the research team wish to use it. The GDPR recognises that it may not be possible to specify all the purposes of the research in advance. Researchers will therefore be expected to allow individuals to give consent only to certain areas of research or to certain parts of the project. Care should also be taken, where necessary, to document in contracts with third party contributors, the consent obligations which they are required to satisfy. The GDPR grants individuals a specific right to withdraw consent at any time, and it must be as easy to withdraw consent as to give it. If consent is the only legal basis for processing, and a research participant were to withdraw that consent , the research team would be obliged to stop processing unless an exemption applied (Refer to Section 9.0 below for further information on GDPR Exemptions).
Legitimate Interest	This lawful basis of processing applies where the processing is necessary for MCRI's legitimate interests or those of a third party, and those interests are not outweighed by the interests and rights of the data subjects. Legitimate interests may be the appropriate legal basis where MCRI is not processing personal data on the basis of consent. The ICO recommends that those considering this basis should undertake a Legitimate Interests Assessment (LIA), comprising three parts. The first part involves identifying the legitimate interests in question; the second determining whether the processing of personal data is necessary to meet those interests; and the third determining whether those interests are outweighed by the rights and interests of the research participants. Whether or not a legitimate interest can be relied upon will depend on the reasonable expectations of the data subjects, based on their relationship with the data controller.
Public Interest Task	This lawful basis of processing applies where the processing is necessary for the performance of a task carried out in the public interest. As a result, personal data can be processed without consent where the processing is necessary for research carried out in the public interest. **It is anticipated that some of MCRI's research activity would fall under this category.**

Legal Obligation	This lawful basis of processing applies where the processing is necessary for the performance of a task carried out in public interest or as required to by law to meet certain regulatory/official requirements and/or legal obligation of the data controller; for example, in order to meet regulatory requirements as set out in the EU Clinical Trial Directive such as safety reporting and archiving of essential study documents. As a result, personal data can be processed without consent where the processing is necessary for research carried out to meet this lawful basis. **It is anticipated that some of MCRI's research activity would fall under this category.**

c) Special Category Data

To process special category personal data, in addition to identifying a lawful basis for processing under Article 6, as described above, researchers must satisfy one of a further set of conditions set out in Article 9. The conditions most relevant to research projects are:

- **Processing with Explicit Consent:** Consent to use special category personal data requires the research team to obtain that consent explicitly. This means that the consent must be provided in the form of an express statement to that effect ('I consent to my data being processed for….'). As above, data subjects must have the right to withdraw their consent at any time.
- **Processing for Scientific Research Purposes**: This will apply so long as technical and organisational measures are in place to provide appropriate safeguards for the rights of research participants, and provided the research is in the public interest.
- **Substantial Public Interest: (Article 9g):** This will apply so long as technical and organisational measures are in place to provide appropriate safeguards for the fundamental rights of research participants, and provided the research is in the necessary reasons of substantial public interest.
- **Processing in the Public Interest in the area of Public Health (Article 9i):** This will apply so long as technical and organisational measures are in place to provide appropriate safeguards which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy.

The processing of personal data for scientific research, substantial public interest and/or processing in the public interest in the area of Public Health are therefore alternatives to the requirement for explicit consent.

d) Transparent Processing

When you are collecting personal data from the individuals concerned (or, in the case of research involving children, from their parents or guardians), you need to be clear, open, and transparent with those individuals, by setting out what you intend to do with their data. Specifically, the GDPR requires that you provide individuals with the following information (this is known as the **prescribed information**):

- The name of the data controller(s) (i.e., MCRI and any co- or joint data controllers if relevant) and the contact details of the local data protection officer and MCRI's data privacy officer
- The purposes for which the data are intended to be processed
- The legal basis for processing

- The intended recipients or categories of recipients with whom the data are to be, or may be, shared
- The fact that the data shall be transferred outside of the European Economic Area (the "EEA") and the safeguards that will apply to that transfer
- The period for which the data will be stored, or, if that is not possible, the criteria that will be used to determine the retention period
- If processing is based on consent, the fact that the data subject has the right to withdraw consent at any time; and
- The existence of the data subjects' rights under the GDPR (right to access their data, right to request rectification or erasure of their data, right to object to processing, right to lodge a complaint).

For research this prescribed information is often provided to data subjects in the form of a privacy notice or participant information and consent form (PICF).

Researchers should consider how they will ensure that all participants (or parents/guardians of child participants) are provided with the correct prescribed information. Whether the prescribed information is provided in a written format, read out to them, or otherwise made available to them will depend on the nature of the research/project and the usefulness of that format to the participants. Above all, the prescribed information should be provided in a user-friendly way that avoids unnecessary jargon, and you should always document that you have provided this, particularly if the prescribed information is read out to data subjects.

8.1.2 Collected for Specified, Explicit and Legitimate Purpose

This data protection principle is clearly consistent with the requirement to provide individuals with certain prescribed information. It follows that where you have obtained personal data for a specified purpose, you should not then be allowed to use it for other purposes (i.e., 'further processing') unless the other purposes are compatible with that original purpose.

However, the GDPR states that the further processing of data for research purposes will be considered compatible with the original purpose for which the data was collected. There is therefore a general presumption that data collected for a non-research purpose may be reused for research purposes. However, it will still be necessary to provide the prescribed information to the data subjects, and to do so before the further processing takes place. It would also be necessary to seek consent for the new purpose if it were the intention to rely on consent as the lawful basis for processing.

Therefore, if a Sponsor of a clinical trial or an investigator of a research project would like to use the personal data gathered for any other purposes than the one defined by the original protocol (e.g., medical data collected to conduct a clinical trial on childhood cancer used to run a study aiming to identify new biomarkers, but which was not foreseen in the clinical trial protocol), it would require a valid legal ground under Article 6 of the GDPR. The chosen legal basis may or may not differ from the legal basis of the primary use, for example, consent.

Where consent is to be used as a legal basis for the processing of personal data for secondary use, the following must be considered:

1. Explicit consent must be obtained

2. The data subject must be informed of the legal basis for processing of personal data; and
3. The data subject is informed of their right to withdraw consent at any time.

8.1.3 Adequate, Relevant and Limited to what is Necessary for the purposes Concerned (Data Minimisation)

This data protection principle is intended to prevent the collection of unnecessary personal data. Given the sensitivities associated with personal data, it follows that no organisation should hold personal data which it does not require. However, this data protection principle also imposes an obligation to ensure that such data is suitable for the researchers' purposes.

The GDPR emphasises that the principle of minimisation applies to all aspects of processing, and not just the amount of data collected. It is therefore important for researchers to consider their obligations under this principle in relation to each aspect of work that involves the processing of personal data.

For example, it may not be necessary for every member of the research team or for collaborators to have access to the full data set and it may be possible to provide information to those persons in an anonymised or pseudonymised form. Access to personal data should always be restricted to those people with a legitimate need to know. Researchers should also consider whether they need to use personal data at all or whether they would be able to meet their objectives with anonymised, aggregated or pseudonymised data.

8.1.4 Accurate and where necessary, Kept Up to Date

This data protection principle relates to the above principle: where data is not kept up-to-date it may cease to be adequate and relevant for the purposes for which it is to be processed.

Accordingly, its retention will cease to be necessary for the purposes for which it was collected. Every reasonable step should be taken to ensure that data, which is inaccurate, having regard to the purposes for which it is processed, is erased, or rectified without delay.

8.1.5 Not to be kept as Identifiable Data for Longer than Necessary

This data protection principle also relates to the third principle above: retaining personal data in an identifiable form for longer than necessarily means the data will no longer be relevant.

The GDPR does not specify how long personal data should be held for, although a specific retention period may be required under other legislation or as a result of regulatory (i.e., ICH-GCP) or policy considerations. In all cases the retention period, or at least its basis and rationale (if not the precise detail), will need to be communicated to the research participants in order to satisfy the requirement for transparency under the first data protection principle. This is generally communicated via the PICF if your project's legal basis for processing is based on consent.

8.1.6 Processed Securely

The GDPR requires researchers to take appropriate **technical and organisational measures** to protect personal data against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. It should be noted that the requirements of the GDPR go beyond the way information is stored and transmitted, relating to every aspect of the processing of personal data.

Security measures should seek to ensure that:

- Only authorised people can access, alter, disclose, or destroy personal data
- Those people only act within the scope of their authority; and
- If personal data is accidentally lost or destroyed it can be recovered to prevent any damage or distress to the individuals concerned.

The level of security that a research project adopts will depend on the risks associated with that project. In particular, the GDPR states that those measures should be appropriate to:

- The nature of the information in question; and
- The harm that might result from its improper use, or from its accidental loss or destruction e.g., Identity fraud, distress at the exposure of private or sensitive information.

The physical security of personal data includes factors such as the quality of doors and locks and whether the premises are protected by alarms etc., however, it also includes how access to the premises is controlled, the supervision of visitors, the disposal of paper waste and the security of portable equipment (e.g., laptops and any storage media or devices). Computer security is constantly evolving and may require specialist advice.

8.1.7 Other Requirements

7.1.7a) Accountability

The GDPR introduces a new requirement for accountability; data controllers must be able to demonstrate that they are complying with the data protection principles and other requirements of the GDPR. It is essential therefore, that researchers reference any Institutional and/or study-specific policies or procedures they will follow in order to comply with data protection requirements. As part of this emphasis on accountability, data controllers are also required to keep records of their processing activities. These records must show:

- The categories of data subject (from whom they collect the data)
- The categories of personal data (what types of data they collect)
- Whether they are processing data on the basis of consent (and if so, how and in what form consent is given), and/or another legal basis under the GDPR
- How their study is complying with the Data Protection Principles set out above
- The categories of recipient (what other parties the data is shared with, if applicable)
- Details of the transfers of personal data outside the EU
- The time limits for erasure
- And a general description of security measures.

Researchers must maintain detailed records as part of their normal data management responsibilities and have a robust Data Management Plan (DMP) developed for their research/project which incorporates the above GDPR accountability requirements.

7.1.7b) Use of Pseudonymisation and Anonymisation

Pseudonymisation, where it would not undermine the function of the research, is mentioned as one example of an appropriate safeguard to reduce the risks to the data subject and help controllers and processors to meet their data protection obligations.

Furthermore, the GDPR expects researchers to use anonymised or pseudonymised data if such data is sufficient for their purposes. It is particularly important therefore that researchers are able to

demonstrate that they have considered the question of whether they could achieve their objectives without the use of fully identifiable personal data.

7.1.7c) Joint Data Controllers

Where two organisations are joint data controllers (i.e., organisations that jointly decide how and why personal data should be used) they need to have a Research Collaboration Agreement in place, and for this to indicate in particular, their respective roles and responsibilities in relation to data subjects, including which controller will be responsible for providing the prescribed information.

This requirement will apply to any research project carried out in collaboration with other institutions where the purposes and means of processing are decided jointly. Researchers should seek advice from the MCRI Legal Team with respect to all such agreements.

7.1.7d) Data Processors

If a researcher is using a third party to collect or process personal data on its behalf (a 'data processor'), it must have a written agreement with that third party which meets the requirements of the GDPR.

Researchers should seek advice from the MCRI Legal Team with respect to all such agreements.

7.1.7e) Data Protection Impact Assessments (DPIA)

The GDPR requires data controllers to complete a Data Protection Impact Assessment (DPIA) for any project that is likely to pose a 'high risk' to the rights and freedoms of individuals. The GDPR does not define 'high-risk' but gives as one example the 'large-scale' processing of special category data.

MCRI recommends that a DPIA is completed for every new project that involves the processing of personal data under the GDPR.

NOTE: The undertaking, preparation, and completion of a DPIA is generally led by the EU based participating/collaborating site (Refer to the next section for further information on MCRI's involvement in a DPIA). However, MCRI researchers and other relevant MCRI staff will be consulted throughout the DPIA process to assist in identifying any potential privacy risks where necessary.

The DPIA involves an assessment of the privacy risks to individuals in the collection, use and disclosure of information. DPIAs help identify privacy risks, foresee problems, and bring forward solutions. Comparable to risk assessments for a data stream, it should cover the flow of data, what the data is used for, how it is managed, and what action is needed.

Furthermore, a DPIA is:

- A tool/process to assist organisations in ensuring that all activities involving personal data are proportionate and necessary
- A tool/process to help with identifying and minimising the privacy risks of new projects, systems, or policies
- A type of impact assessment conducted by an organisation, auditing its own processes to see how these processes affect or might compromise the privacy of the individuals whose data it holds, collects, or processes.

7.1.7f) What is MCRI Researcher's involvement in a DPIA?

Whilst the undertaking, preparation, and completion of a DPIA may be led by the EU participating/collaborating site within your research/project, MCRI researchers, however, will need

to be in a position to demonstrate that they have proactively addressed the data protection implications of their research/projects, in order to comply with the requirements for accountability and privacy by design. Furthermore, it is important to note that the size and level of detail in a DPIA should be proportionate to the scale of the project and the related privacy risk. Account should be taken of the nature, scope, context, and purpose of the data processing.

There may be some instances whereby EU participants self-refer into MCRI research projects and there are no participating/collaborating sites based within the EU. In these instances, it will be the responsibility of the Australian Principal investigator, with the assistance of the MCRI Legal Team and Privacy Officer (referred to in the GDPR as the "Data Protection Officer (DPO)"), to complete the DPIA for their study and ensure that it meets the requirements of the GDPR.

In order to fulfil the requirement of a DPIA, MCRI researchers must first develop robust and concise Data Management Plans (DMP) for their studies/projects, documenting appropriate technical and organisational measures to safeguard personal and special categories of data. Typically, a DMP outlines what research data will be created during the course of a research project and how it will be created, plans for sharing and preserving the data and any restrictions that may need to be applied. The DMP must also include a concise description of how you collect, store, use and process personal and special category data. The following also needs to be addressed in each DMP:

- The role of personal data in the project
- Identify any risks to privacy within your project
- Identify any risks to privacy to Data Subjects
- A description of the processing operations and purpose
- Why the processing of personal data is necessary and proportional for the purposes of your project
- The information flow of the data collected
- A description of who has access to the data and how the data will be stored/secured
- A description of any transfers of data outside the EEA
- A statement on how to monitor and log any future requests for access to the data i.e., data sharing requests/data transfer methods.

Whilst a DPIA's main focus is on the organisation's processing activities around Personal Data and minimising risks associated with its collection and processing, a DMP outlines the research projects entire life-cycle including how data are to be handled both during a research project and after a project is completed.

The CEBU Data Management Plan Template is available for use to MCRI Researchers.

MCRI is in the process of developing a suite of resources around Data Protection and GDPR compliance, including a Data Protection Impact Assessment (DPIA) SOP. Until this is available, researchers should seek advice from the MCTC Team and MCRI Legal Team with respect to all DPIAs.

9. Can Personal Data be transferred to a Country/Territory outside the EEA?

There is a general prohibition on transfers of personal data outside of the EEA unless these transfers are subject to quite narrowly prescribed conditions and safeguards, such as:

- The transfer is to an "adequate jurisdiction" (i.e., one declared by the EU Commission to adequately protect personal data). Refer to section 8.1 for further information.
- The party transferring the personal data has entered into a binding agreement with the party receiving the personal data which incorporates the "standard contractual (model) clauses" approved by the EU Commission, or
- The data subject has explicitly consented to the transfer (having been informed of the possible risks of such transfers).

Researchers should seek advice from the MCRI Legal Team for advice on all research-related agreements, including for projects involving transfers of personal data outside the EEA under standard contractual clauses, or otherwise.

9.1 Data Transfers to 'Adequate Jurisdictions'

Data transfers to adequate jurisdictions as declared by the EU Commission to adequately protect personal data, include the following jurisdictions:

- All EU member states including Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, the United Kingdom and including EFTA states Iceland, Norway, and Liechtenstein.
- As of February 2019, the ICO has made a full finding of adequacy regarding the following countries and territories: Andorra, Argentina, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland, and Uruguay.
- The ICO has made partial findings of adequacy about Japan, Canada, and the USA.
    - The adequacy finding for Japan only covers private sector organisations.
    - The adequacy finding for Canada only covers data that is subject to Canada's Personal Information Protection and Electronic Documents Act (PIPEDA). Not all data is subject to PIPEDA.
    - The adequacy finding for the USA is only for personal data transfers covered by the EU-US Privacy Shield framework. Refer to Section 8b below for further information on the EU-US Privacy Shield.
- To date, the EU Commission has not declared Australia to be an "adequate jurisdiction".

8a) Cloud Service Providers

Researchers need to bear in mind that using international cloud-based services e.g., Dropbox, may involve a transfer of personal data outside the EEA. Even if the service in question has signed up to the EU-US Privacy Shield (see Section 8b below), it may not be appropriate to use such a service, since the terms and conditions tend to be one-sided, and are unlikely to be sufficient to enable MCRI to meet all its obligations under the GDPR. The risks will be greater where the personal data involved is confidential or sensitive. You therefore need to think carefully about whether you could use an alternative service that complies fully with the GDPR or whether you could use the service without sharing personal data.

Researchers are not authorised to sign up MCRI to the terms and conditions of any service providers (including cloud-based service providers) and all contracts with service providers must be reviewed by MCRI Legal and executed by an authorised officer of the institute.

8b) Privacy Shield

The EU-U.S. and Swiss-U.S. Privacy Shield Frameworks were designed by the U.S. Department of Commerce, and the European Commission and Swiss Administration, respectively, to provide companies on both sides of the Atlantic with a mechanism to comply with data protection requirements when transferring personal data from the EU and Switzerland to the US.
Therefore, a data transfer from the EU directly to a US Organisation (bypassing MCRI) that has been certified under the EU-US Privacy Shield Framework will be regarded as legal under the GDPR. The list of organisations that are certified under the Privacy Shield can be searched here.

10. The GDPR's Research Exemptions

The principles of Data Protection do not apply to anonymous information. Anonymous information is information that does not relate to an identified or identifiable natural person, or information that is rendered anonymous in such a manner that the Data Subject is not or no longer identifiable. Pseudonymized personal data, however, are not exempt (e.g., encrypted data where the process can be reversed via an encryption key).

The GDPR acknowledges the need to facilitate different types of research, citing scientific and historical research, statistical research, and archiving in the public interest (Article 89 GDPR). However, it does not contain a formal definition of what constitutes scientific research. It applies a wide definition to the notion of research, stating that "the processing of personal data for 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."

The GDPR sets out a number of exemptions to obligations relating to the processing of personal data where it is necessary for scientific research. The exemptions may only be relied upon where an organisation is complying with the requirement for appropriate safeguards under Article 89. In particular, the safeguards must ensure that technical and organisational measures are in place which ensure the principle of data minimisation.

Some exemptions are expressly set out in the GDPR.

9.1 Exemption – Processing of Special Category Data

As noted above, it is lawful to process special categories of personal data (including health data) where the processing is necessary for scientific research purposes, and adequate safeguards are in place.

9.2 Exemption - Reuse of Personal Data for Research

As noted above, one of the Data Protection Principles states that "personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those processes".

The Data Protection Principles go on to say that further processing for scientific research purposes will not be considered incompatible with the initial purposes, provided that appropriate safeguards are in place.
Care must still be taken to ensure that any further use is compliant with all other relevant obligations under the GDPR e.g., the Data Protection Principle of transparency, and the need to have a lawful basis for processing.

Regarding the secondary or further use of data collected during clinical trials, aligning with the CTR must also be considered. In this case, the CTR states that *"[i]t is appropriate that universities and other research institutions, under certain circumstances that are in accordance with the applicable law on data protection, be able to collect data from clinical trials to be used for future scientific research, for example for medical, natural or social sciences research purposes. In order to collect data for such purposes it is necessary that the subject gives consent to use his or her data outside the protocol of the clinical trial and has the right to withdraw that consent at any time. It is also necessary that research projects based on such data be made subject to reviews that are appropriate for research on human data, for example on ethical aspects, before being conducted."* Here, the CTR refers to EU data protection law as the framework for further processing of personal data, now being the GDPR.

The GDPR adds to this by the stating in Recital 33 GDPR that *"it is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection. Therefore, data subjects should be allowed to give their consent to certain areas of scientific research when in keeping with recognised ethical standards for scientific research. Data subjects should have the opportunity to give their consent only to certain areas of research or parts of research projects to the extent allowed by the intended purpose."*

The scope of the notion of research under the GDPR is wide. Article 89 GDPR functions by setting a baseline in that requires that any derogation is subject to the existence of appropriate safeguards for the rights and freedoms of data subjects. Here, the GDPR stresses that safeguards shall include:

- Data minimization
- Technical and organisational measures
- Privacy by Design and by Default
- Pseudonymization/further processing.

If the above safeguards are in place, derogations to the following points may be applied:

i) Further processing and storage limitation (Articles 5(1)(b) and (e) GDPR)
ii) Processing of special categories of data (Article 9(2)(j) GDPR)
iii) Information provided by third parties (Article 14(5)(b) GDPR)
iv) Right to erasure (Article 17(3)(d) GDPR)
v) Right to object (Article 21(6) GDPR).

10.1 Exemption - Retention

The fifth data protection principle requires that data be kept as identifiable data for no longer than is necessary to meet the purposes for which the data is processed. However, personal data which are processed for research purposes may be kept for 'longer'. The GDPR does not currently define what is meant by 'longer than necessary'.

Advice to researchers is to clearly state in your participant information and consent forms (PICFs), the minimum retention period of your data, e.g., the information will be retained for a period of 25 years. Any hard copy information will be shredded and disposed of at the end of this period. The electronic data will be deleted/destroyed in a secure manner.

10.2 Exemption – Transparency as to processing

If personal data processed for research has been collected from a third party and not directly from the individuals concerned, it will not be necessary to provide the prescribed information as to how personal data will be used directly to each individual if doing so would require a disproportionate effort or if it would prevent or seriously impair the achievement of the research objectives. Even so, you must still

make the prescribed information publicly available. However, even where this exemption applies, the data controller must nevertheless make the information publicly available (such as through a privacy notice) and take appropriate measures to protect the data subject's rights and interests.

10.3 Individual Rights and exemptions

The GDPR grants individuals new or improved rights in relation to their personal data, including:

- The right to access the data
- The right to object to processing
- The right to request that the data be deleted (i.e., *The right to be 'forgotten'*)
- The right to request that the processing of the data be restricted; and
- The right to request the rectification of inaccurate or incomplete data.

However, these rights are not absolute. Where personal data is processed solely for the purposes of research, there are circumstances where these rights will not apply. For example, in relation to the 'right to be forgotten', MCRI would not be legally required to give effect to that right to the extent that doing so would prevent or seriously impair the achievement of the research purpose.

Should MCRI researchers receive requests of the kind described above, they should refer them to the MCRI Privacy Officer for consideration.

Please also refer to the MCRI Data Subjects Rights SOP for further information.

NOTE: The above exemptions are only available where the processing satisfies the requirement for appropriate safeguards, as described above in Section 9.1.

11. Practical Considerations

This section is intended to highlight some of the issues that researchers may need to consider at different stages of their research/project. It is extremely difficult to highlight all of the issues which may arise during the course of every project and, accordingly, this section is not exhaustive.

- **Third-Party Processing** – When researchers are using a third party to collect or process personal data on their behalf (a data processor), they need to seek advice from MCRI Legal Team in relation to putting in place an agreement with that third party which meets all of the requirements of the GDPR in relation to data processors, and which is otherwise acceptable to MCRI.

- **Security** – Have researchers considered appropriate security measures and implemented a policy for handling personal data? Consider speaking with CEBU for REDCap queries and MCRI IT for security matters to determine whether the security measures you have implemented are appropriate for your research.

- **Sharing** – If researchers are intending to share access to personal data with third parties, then this transfer will need to be governed by a written agreement with those parties, setting out the conditions on which the data is made available. The data transfer agreement will include appropriate, depending on the nature of the data and whether it has been pseudonymised or anonymised (i.e., fully de-identified). As noted above, pseudonymized data counts as personal data under the GDPR; only anonymized data are excluded from the requirements of the GDPR. Researchers must therefore seek advice from the MCRI Legal Team accordingly before agreeing to share any data.

Researchers should also want to refer to the MCTC Data Sharing and Access SOP for further information regarding institutional data sharing requirements for MCRI sponsored Investigator-Initiated Clinical Trials.

- **Data Management Plans / Data Protection Impact Assessments (DPIA)** – Have researchers developed a robust and concise Data Management Plan for their research/project? This is an important document to enable MCRI to demonstrate compliance with the GDPR. It will also assist MCRI's collaborating/partnering organisations based in the EU to complete their mandatory DPIA. In some cases, research may not begin until a DMP and DPIA has been undertaken and sign-off.

  The CEBU Data Management Plan Template is available for use to MCRI Researchers.

11.1 GDPR Examples

To assist researchers with interpreting the various GDPR Regulations and Articles, a number of examples and scenarios are provided in Appendix 1.

11.2 GDPR Cheat Sheet and Data Protection Checklist

To assist researchers in verifying whether their research complies with the GDPR and data protection requirements, a GDPR Cheat Sheet is provided in Appendix 2 and a Data Protection Checklist has been developed.

12. Conclusion

The GDPR and the Australian Privacy Act 1988 (Cth) share many common features. Under both legislative frameworks, researchers must implement a "privacy by design" approach and be able to demonstrate compliance with privacy principles and obligations.

However, there are some differences which must be carefully considered when planning and conducting a research study involving the collection of personal data from participants in the EU.

13. Further Information

MCRI Legal Team legal@mcri.edu.au	Melbourne Children's Trial Centre (MCTC) MCTC@mcri.edu.au

14. Applicable Supporting Documents

- MCTC107 GDPR Information Sheet and Quick Facts Guideline
- MCTC108 GDPR Data Protection Checklist
- MCTC Data Sharing and Access SOP
- CEBU Data Management Plan Template

References

1. GDPR - Regulation (EU) 2016/679 of the European Parliament and the of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

2. Directive 2001/20/EC of the European Parliament and of the Council of the 4 April 2001 on the approximation of the laws, regulations and administrative provisions of the Member States relating to the implementation pf good clinical practice in the conduct of clinical trials on medicinal products for human use.

3. REGULATION (EU) No 536/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 16 April 2014 on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC

4. A Guide to European Data Protection. Hemmingsen, L.T. 2018.

5. UK's Information Commissioner's Office (ICO) website: https://ico.org.uk/

6. Fundamentals of Clinical Data Science; Chapter 5 – The EU's General Data Protection Regulation (GDPR) in a Research Context. Christopher F Mondschein and Cosimo Monda. 2019.

7. Question and Answers on the interplay between the Clinical Trials Regulation and the General Data Protection Regulation. European Commission Directorate-General for Health and Food Safety.

Appendix 1: GDPR Examples

Example: How Does the GDPR Apply to Clinical Research in the EU and Beyond?

An Australian citizen enrols in a clinical trial in Australia that requires her to wear a device that collects her health information. She travels to the EU while participating in that study and continues to wear her device, which continues to collect her health information. All personal data collected and transferred to Australia while that participant is in the EU is subject to the GDPR.

On the other side of the coin, the GDPR generally will not apply to EU citizens enrolling in an Australian clinical trial while located in Australia. However, if the clinical trial is being advertised in the EU, or if participants are followed or follow-up care is provided when participants return to the EU, then the GDPR may apply.

Example: Can we change our lawful basis?

An organisation decided to process Personal Data on the basis of consent and obtained consent from individuals. An individual subsequently decided to withdraw their consent to the processing of their data, as is their right. However, the organisation wanted to keep processing the data so decided to continue the processing on the basis of legitimate interests.

Even if it could have originally relied on a different legal basis (e.g., legitimate interests), the organisation cannot do so at a later date – it cannot switch basis when it realised that the original chosen basis was inappropriate (in this case, because it did not want to cease processing once consent was withdrawn). It should have made it clear to the individual from the start that it was processing on the basis of legitimate interests and consent (rather than consent alone). It is contrary to the GDPR, particularly the Data Protection Principle of "transparency" to represent to the individual that their data was being processed solely based on their consent, and to then seek to continue to process the data once consent has been withdrawn. The organisation must therefore stop processing when the individual withdraws consent if consent was the only legal basis initially nominated for the processing.

Example: When could we be processing too much Personal Data?

An employer holds details of the blood groups of some of its employees. These employees do hazardous work, and the information is needed in case of accident. The employer has in place safety procedures to help prevent accidents so it may be that this data is never needed, but it still needs to hold this information in case of emergency.

If the employer holds the blood groups of the rest of the workforce, though, such information is likely to be irrelevant and excessive as they do not engage in the same hazardous work.

Example: What about records of mistakes?

1. *A misdiagnosis of a medical condition continues to be held as part of a patient's medical records even after the diagnosis is corrected, because it is relevant for the purpose of explaining treatment given to the patient, or for other health problems.*

   It is acceptable to keep records of mistakes, provided those records are not misleading about the facts. You may need to add a note to make clear that a mistake was made.

Example: Does Personal Data always have to be up to Date?

An individual places a one-off order with an organisation. The organisation will probably have good reason to retain a record of the order for a certain period for accounting reasons and because of possible complaints. However, this does not mean that it has to regularly check that the customer is still living at the same address.

You do not need to update personal data if this would defeat the purpose of the processing. For example, if you hold personal data only for statistical, historical, or other research reasons, updating the data might defeat that purpose.

In some cases, it is reasonable to rely on the individual to tell you when their personal data has changed, such as when they change address or other contact details. It may be sensible to periodically ask individuals to update their own details, but you do not need to take extreme measures to ensure your records are up to date, unless there is a corresponding privacy risk which justifies this.

Example: What about Adequacy and relevance of opinions?

A GP's record may hold only a letter from a consultant and it will be the hospital file that contains greater detail. In this case, the record of the consultant's opinion should contain enough information to enable detailed records to be traced.

A record of an opinion is not necessarily inadequate or irrelevant personal data just because the individual disagrees with it or thinks it has not taken account of information they think is important.

However, in order to be adequate, your records should make clear that it is opinion rather than fact. The record of the opinion (or of the context it is held in) should also contain enough information to enable a reader to interpret it correctly. For example, it should state the date and the author's name and position.

If an opinion is likely to be controversial or very sensitive, or if it will have a significant impact when used or disclosed, it is even more important to state the circumstances or the evidence it is based on. If a record contains an opinion that summarises more detailed records held elsewhere, you should make this clear.

Example: Compatible Purposes for "Re-Use" of Collected Data

A GP discloses his patient list to his wife, who runs a travel agency, so that she can offer special holiday deals to patients needing recuperation.

Disclosing the information for this purpose would be incompatible with the purposes for which it was obtained.

Example: International Transfers

A subsidiary company in the EU uses a centralized human resources system in India belonging to its parent company to store information about its employees. Appropriate safeguards need to be put in place to frame the transfers of data from the European Union based subsidiary to the parent company in India.

Example: How long can we keep personal data for archiving, research, or statistical purposes?

You can keep personal data indefinitely if you are holding it only for:

- archiving purposes in the public interest
- scientific or historical research purposes
- or statistical purposes.

Although the general rule is that you cannot hold personal data indefinitely 'just in case' it might be useful in future, there is an inbuilt exception if you are keeping it for these archiving, research or statistical purposes.

You must have appropriate safeguards in place to protect individuals. For example, pseudonymisation may be appropriate in some cases.

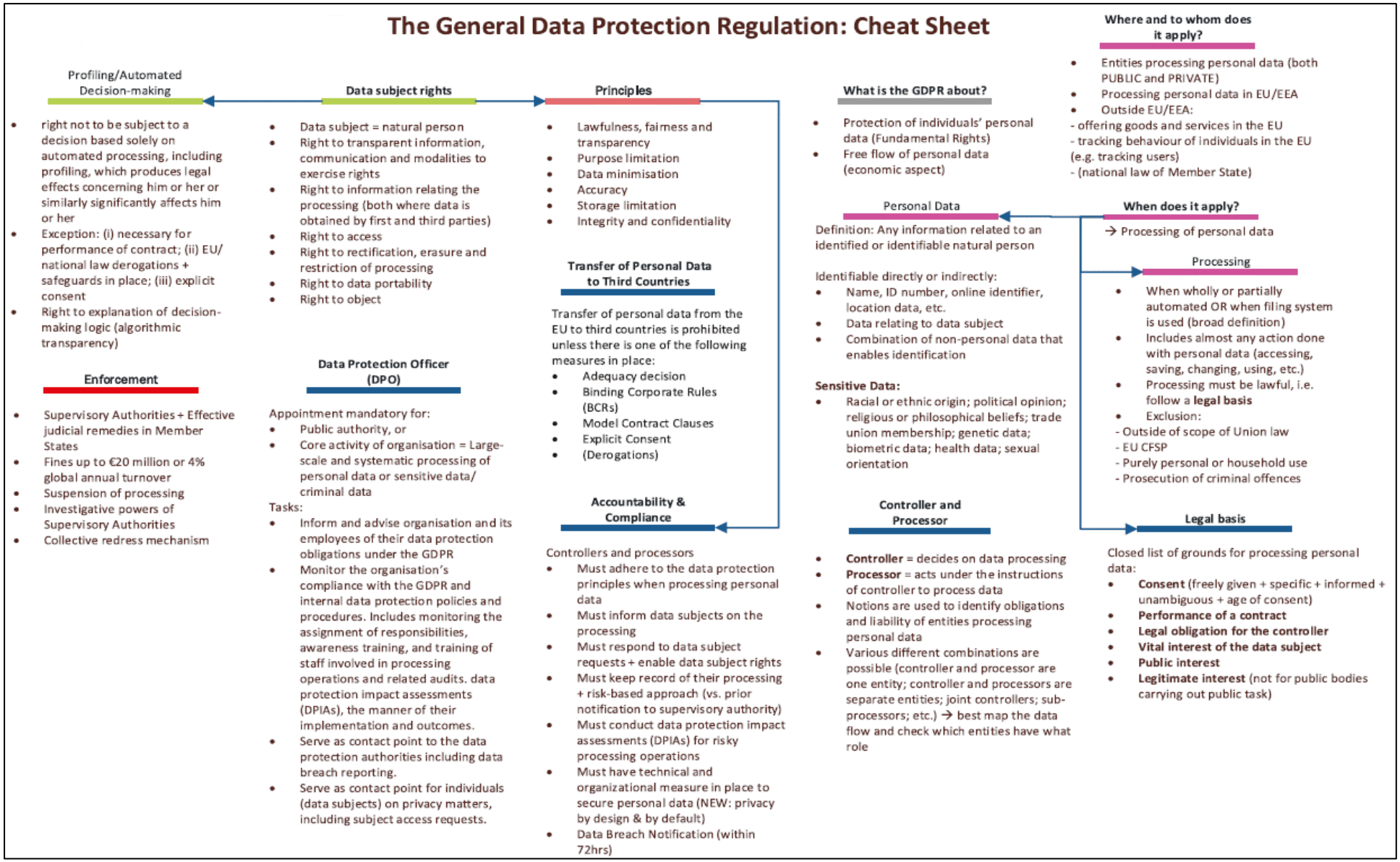
This must be your only purpose. If you justify indefinite retention on this basis, you cannot later use that data for another purpose - in particular for any decisions affecting particular individuals. This does not prevent other organisations from accessing public archives, but they must ensure their own collection and use of the personal data complies with the principles.

Example: You have received a Data Subject Request – do you have to explain the contents of the information/data you send to the Individual?

You receive a subject access request from someone whose English comprehension skills are quite poor. You send a response, and they ask you to translate the information you sent them.

You are not required to do this even if the person who receives it cannot understand all of it because it can be understood by the average person. However, it is good practice for you to help individuals understand the information you hold about them.

Appendix 3: European Centre on Privacy and Cybersecurity (ECPC) – GDPR Cheat Sheet



Reference: Fundamentals of Clinical Data Science; Chapter 5 – The EU's General Data Protection Regulation (GDPR) in a Research Context. Christopher F Mondschein and Cosimo Monda. 2019