GDPR Guideline for Researchers: Information Sheet & Quick Facts

European Union General Data Protection Regulation (GDPR)

The European Union's (EU) General Data Protection Regulation (GDPR) was enacted on the 25th May 2018. The regulation applies to any organisation processing personal data of individuals located in the EU (regardless of whether the organisation is located in the EU or outside the EU, such as in Australia).

If you are unsure whether the GDPR applies to your particular study or scenario, and if so how to ensure compliance, 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.

Note: this information sheet and quick facts document is a summary of a much more comprehensive document available for MCRI Researchers entitled: *Principals of the General Data Protection Regulation (GDPR) & Data Protection in a Research Context: A Guideline for Researchers.*

What is the GDPR?

The General Data Protection Regulation (GDPR) establishes and enhances protections for the privacy and security of personal data about individuals within the EU. It places restrictions on handling personal data and delineates the responsibilities and obligations of organisations processing personal data.

GDPR Terminology

Data Controller	The person or legal entity responsible for determining the purpose and means of processing personal data. ➢ For clinical trials (CTs), this is the sponsor. ➢ For observational research studies, this will be the party which designs, manages, and coordinates the study (i.e., the party making the decisions about the collection and use of personal data in the study) ➢ Another entity may be considered a joint controller (e.g., a CRO or a collaborator in a clinical trial or other research study).
Data Processor	The person or entity who processes personal data for the Data Controller E.g., a third-party service provider engaged to store or otherwise process the data on instruction by the Data Controller.
Data Subject	The individual(s) within the EU whose personal data is being collected and processed. For research studies, this is the participant. It may also include other individuals such as site investigators and study team members who are involved in the study.
Data Protection Officer (DPO)	The person who advises the organisation on its data protection strategy and implementation in compliance with the GDPR requirements. The DPO is also the contact point for Data Subjects and the organisation's regulatory authority
Personal Data	Any information which relates to an identified or identifiable living individual located in the EU who can be identified from that information, whether directly or indirectly, and in particular by reference to an identifier. An identifier 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.

What does the GDPR Cover?

Under the GDPR, personal data is "any information relating to an identified or identifiable natural person" (AKA the "data subject"). Even coded data (or "pseudonymized data") is considered personal data that would be subject to the protections of the GDPR. Data that has been fully anonymized is not covered by the GDPR.

The GDPR further defines special categories of data, called "sensitive personal data," which are subject to stricter regulation. This would include data typically collected in a clinical trial, including health data, genetic data, and biometric data. This category also includes racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sex life or sexual orientation.

How does the GDPR Apply to Research in the EU and Beyond?

The GDPR is intended to cover EU personal data, including data processed for clinical trials, medical research projects and registries and applies directly to organisations located in the EU, Iceland, Liechtenstein, and Norway. It also applies to the processing of personal data by a controller or processor not located in the EU when the data processing is related to:

(a) Offering goods or services to participants in the EU, or

(b) Monitoring of behaviour of participants within in the EU, as far as their behaviour takes place in the EU.

It applies to anyone while in the EU, not just EU residents. This means that the GDPR may affect Australian research projects even if the research is not conducted in the EU.

Example: An Australian citizen enrols in an Australian clinical trial 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.

Conversely, 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.

How are Research Participants Informed of GDPR Data Privacy Requirements?

If the study is subject to the GDPR, detailed data privacy information must be provided to participants. This data privacy notice may be included in the informed consent form (preferred option), a data privacy addendum to the consent form, or a separate letter to participants. The way in which MCRI handles personal data (including in compliance with the GDPR) is also set out at a general level in our MCRI General Privacy Policy published on our website. The good news is that most Australian research consent forms already include most of the information which research participants are required to be given to ensure compliance with the GDPR.

The elements related to data privacy that must be included in the participant information and consent form include:

- Identity and the contact information of the data controller (also referred as the sponsor for clinical trials)
- Contact information for the data protection officer (DPO) (generally the EU DPO will be listed, but the details for MCRI's Privacy Officer may also need to be included)
- Listing of any special categories of personal data that will be collected for the study, such as:
    - Age, sex, ethnic and racial background

  - Health and medical conditions including past medical history
  - Study procedures and response to procedures
  - Information related to the participant's sex life
  - Biological samples (e.g., urine, blood, tissue, and the results learned from analysing them).
- An explanation as to the legal basis for the processing (e.g., whether the data is being processed based on consent and/or other legal bases set out under the GDPR)
- Informing participants of the existing of their Individual Data Subject Rights, and how they may be exercised:
  - The right to access the data
  - The right to object to processing
  - The right to erasure (i.e., The right to be 'forgotten')
  - The right to request that the processing of the data be restricted
  - The right to request the rectification of inaccurate or incomplete data; and
  - The right to file a complaint with the Data Protection Authority.
- Transfer of Data (Outside the EU and if also transferring the data to others): A statement about the circumstances under which it will be transferred and safety measures taken to protect the data (e.g., data are encoded).
  - For any data being transferred outside of the EU to Australia (i.e., hosted in an Australian database): A statement that the countries who are receiving the data may not have had their data protection level confirmed as adequate by the European Commission, and any safety measures taken to protect data privacy rights. *Note: The EU has not confirmed that Australia has an adequate level of data protection, and a review of the Privacy Act is underway which may address this.*
- Retention of Data: a statement describing how long the data will be maintained/stored.

The GDPR's Research Exemption

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). It does not contain a formal definition of what constitutes "scientific research", but it is reasonable to interpret that term broadly.

There are a number of exemptions from specific duties and obligations under the GDPR for processing that is carried out for the sole purpose of research.

Exemption - Reuse of Personal Data for Research

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.

When relying on this exemption for future processing, 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, as well as all the standard requirements needed for secondary use of collected data i.e., ethics committee approvals and re-consenting of participant's (if applicable).

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. 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 conditions must be met:

1. Explicit consent must be obtained, unless a waiver of consent is granted
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.

Exemption - Retention

One of the GDPR data protection principles 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.

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, e.g., from a Government Agency, it will not be necessary to provide the prescribed information 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. For example, MCRI is obtaining personal data from the RCH EMR for research purposes under a waiver of consent that has been approved by the RCH HREC. In this case, this is feasible so long as you publicise that you are undertaking the research (i.e., via a privacy notice).

Exemption - Individual Data Subject Rights

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, if by doing so, it would prevent or seriously impair the achievement of the research purpose. In a medical research project setting, should a participant request that their data be withdrawn from a project, the data collected up until that point may not be required to be deleted, even if the participant expressly states that it is his/her "right to be forgotten", as deleting such information may seriously impact the integrity of the data or impair the achievement of the research purpose.

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

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. 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 to enter into an agreement with that third party to ensure the information is processed in accordance with MCRI's legal obligations.

- **Security** – Have researchers considered appropriate security measures and implemented a policy for handling personal data?

- **Data Sharing** – If researchers are intending to share access to personal data, then they are required by law to enter into a written agreement with those parties (i.e., Data Sharing Agreement), setting out the conditions on which the data is made available. Where it is possible, any personal data that is to be shared/transferred should always be anonymised, therefore the GDPR does not apply. Note: Pseudonymized data count as personal data; only anonymized data are excluded from the requirements of the GDPR Regulation. Researchers should seek advice from the MCRI Legal Team accordingly before agreeing to share any data.
    - Researchers may 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 will assist collaborating/partnering Institutions based in the EU complete their mandatory DPIA. In some cases, research may not begin until a DMP and DPIA have been undertaken and sign-off.

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

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 1 and a Data Protection Checklist has been developed.

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.

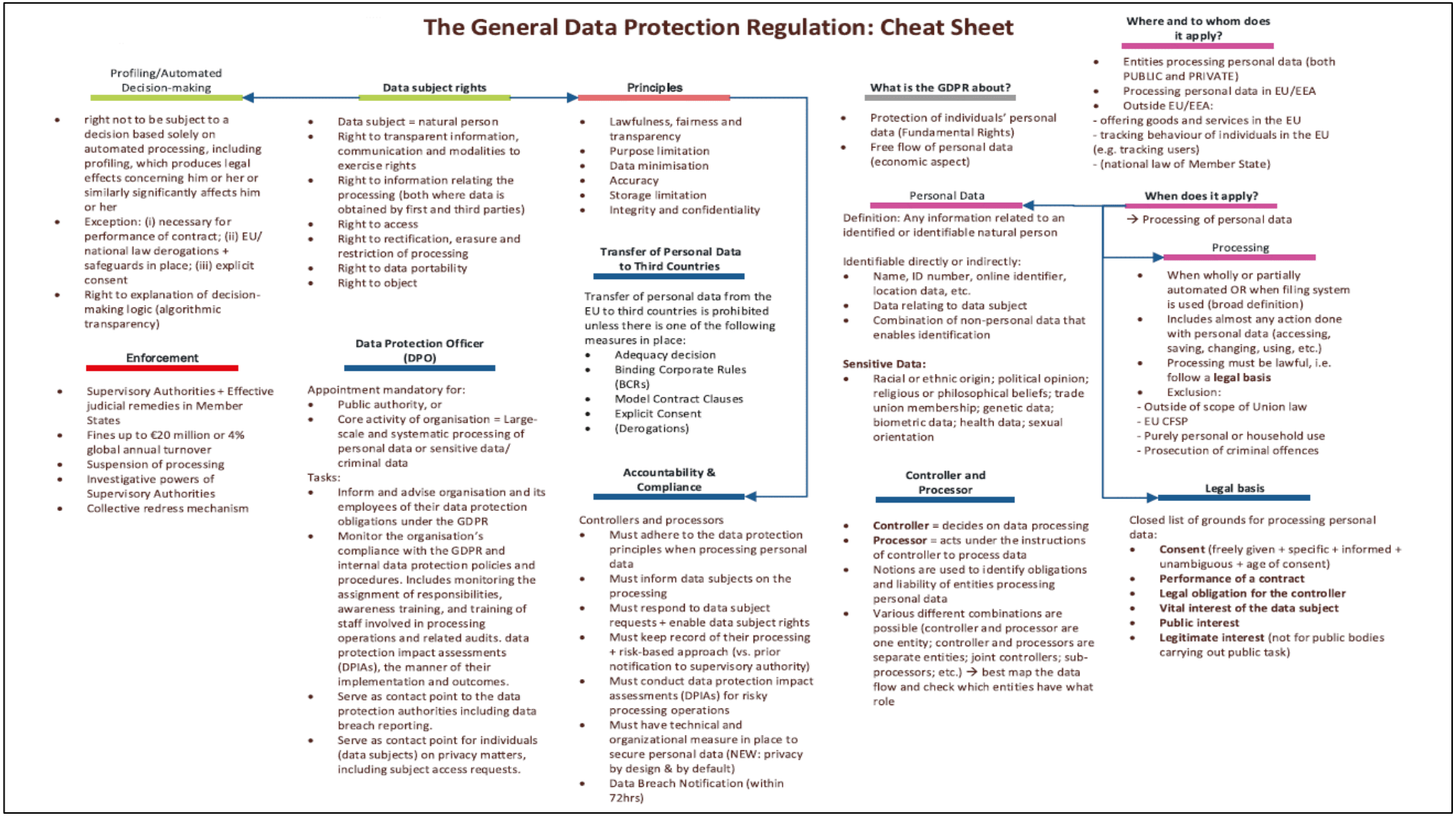
Further Information

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

Applicable Supporting Documents

- MCTC106 Principals of the General Data Protection Regulation (GDPR) & Data Protection in a Research Context
- MCTC108 GDPR Data Protection Checklist
- MCTC Data Sharing and Access SOP
- CEBU Data Management Plan Template

Appendix 1: 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.