**Overview:**

Researchers need to ensure data processing is **lawful, fair and transparent** and adhere to the 5 R:s:

- Respect personal data
- Reduce data collected
- Restrict access to data
- Review and delete data (including the "right to be forgotten")
- Removed identities if possible

In order to use personal data for research both the legal basis (GDPR) and the ethical basis (informed consent) need to be satisfied. In general, good research practice already meets most GDPR regulation. Greatest implications are around transparency and accountability. GDPR does not apply to anonymised data. It does permit "Big Data" research where this methodological approach is necessary and in general facilitates the conduct of research.

In the case of research, data subjects are usually the research participants and data controllers are the researchers (but could include, for example, the clinical trials unit).

If in doubt, contact your local Data Protection Officer (DPO).

The key relevant changes brought by the GRPD to research include its:

- wider global scope – therefore emphasising importance of international studies in child and adolescent health such that GRPD covers the data of all EU residents, regardless of location of processing, and the processing of any data within the EU, regardless of the country of origin of the data.
- broader definition of personal data – now including pseudo-anonymised data
- broader definition of special category data with biometric and genetic data included
- increased emphasis on protection of children and young people (CYP), in particular the requirement to provide accessible information
- higher standards for consent (when needed – however although consent is a potential lawful ground under which to process personal data, it is generally recommended that researchers avoid using consent as their legal basis in which case they do not need to adhere to GDRP consent requirements, only those usually set out by research ethics ).
- increase in research participant data rights (however, some of these rights may be overridden under GDPR regulation as long as appropriate safeguards (including transparency and accountability) are in place).
- increased accountability at organisational level
- need for layers of transparent and accessible information for research participants.
- The "right to be forgotten/ to erasure" and research exemptions

A research participant has the right to request personal data be erased either when he/she withdraws consent, or when the data are no longer needed for the initial purpose for which they were collected. However, if adhering to this request would render the achievements of the research objectives impossible or improbable, the researcher does not have to comply with this request.

**Practical steps for researchers processing data:**

Continue to adhere to best research governance practice AND all additional legal requirements AND

1. Decide and clearly document the **lawful grounds under which you are processing personal data**

    a. Out of the six possible grounds set out in GDPR, research under universities/ NHS/ research councils is likely to be conducted in "public interest".
2. Decide and clearly document the **lawful condition under which you are processing special category data** AND **ensure suitable and specific safeguards are met including the subject's right to data protection**.
    a. Out of ten possible lawful conditions set out in GDPR for processing special category data and additional conditions outlined in the Data Protection Act 2018, the most relevant lawful condition for processing special category data for research purposes is likely to be: "… in the public interest, scientific or historical research purposes or statistical purposes..".
3. **Undertake a Data Protection Impact Assessment** (DPIA) before project start and prior to contract negotiations where there remains time to modify project design. They should be updated following any significant project changes
    a. There are two types: general/ professional and research. Most researchers will be concerned with the latter.
    b. DPIA is the systematic analysis, identification and proposed mitigation of the data protection risks of a project (for research example, see:[1])
4. **Provide a hierarchy of accessible, developmentally appropriate information** e.g. age-appropriate information sheets and privacy notices
    a. **Privacy notices** These should be presented at each institutional layer – from a wider institutional notice, down to "local" project-specific privacy notices included in the project participant information sheets (for example, see: [2]). Where seeking both parental and CYP consent, a privacy notice for both parents and CYP should be provided They should clearly describe the following information:
        i. what categories of personal data are being collected and for what reason(s)
        ii. duration for which these data will be held.
        iii. lawful basis of processing.
    b. Privacy notices for under 18 years must:
        i. Outline the rights of the CYP over their data in understandable language (aim for reading age of 14 years,
        ii. Include child friendly ways of presenting information e.g. infographics
        iii. describe data processing risks
5. **Review and document consent procedures** according to usual research ethics guidance. GDPR consent recommendations states consent needs to:
    a. be freely given, informed, unambiguous, specific and by a clear affirmative action
    b. be explicit when concerning special categories of data e.g. planned/specific investigations for biological samples
    c. Preferably be written without use of pre-ticked opt-in boxes
    d. Include a statement on data sharing and future uses
6. **Address the principles of purpose and storage limitation or explicitly state and record reason(s) for exemption**. Of note, subject to appropriate safeguards, GDPR allows processing of personal data beyond the purposes and the duration for which data were originally collected.
    a. Clearly identify, document, communicate and review purpose(s) for data processing, future data collection (for example in longitudinal cohort studies) and data retention.
    b. If data are used for a new purpose, check this is compatible with original purpose or specific consent is needed for the new purpose

c. Compatible purposes where new consent to process the data is not required include:
    i. Archiving purposes in the public interest
    ii. Scientific or historical research purposes (in practice this means that subject to appropriate safeguards, personal data can be held indefinitely if collected for research purposes)
    Statistical purposes

7. **Ensure data Minimisation**
    a. Only collect necessary data
    b. Delete unnecessary data (important and not previously emphasised as part of usual data processing procedures)
    c. Where possible anonymise data, if not possible pseudo-anonymise
8. **Maintain data accuracy**
9. **Clearly document data sharing agreements**, including storage limitation e.g. between different collaborating laboratories
    a. GDPR allows for more than one data controller where the data controller is responsible for processing the data.
    b. Data may be transferred to countries outside of the EU subject to fulfilling a number of strict criteria.
        i. Researchers may share anonmyised data with other researchers, idenfitiable data with participants consent. If data are shared for a new purpose, participants should be informed, in line with GDPR transparency.
10. **Adhere to principles of integrity and confidentiality**
11. **Accountability** – personal and organisational
    a. Have clear out of office response for data requests, for example:
        *'I will be away from X to Y date with no access to email. If you would like to submit a request for use any of your individual rights under data protection legislation (e.g. the right of access to your personal data), please contact X."*
    b. Report data breeches (incidents or near misses) within 72 hours to the appropriate supervisory authority.

**References**

1. University College London. Data Protection Impact Assessment, https://www.ucl.ac.uk/legal-services/ucl-general-data-protection-regulation-gdpr/guidance-notices-ucl-staff/data-protection-impact (2018, accessed 27th Jan 2019).
2. University College London. Privacy Notice, https://www.ucl.ac.uk/legal-services/ucl-general-data-protection-regulation-gdpr/guidance-notices-ucl-staff/guidance-writing-privacy (2018, accessed 27th Jan 2019).