# Data Protection Guidance for Researchers

The following is meant to be a practical guide to handling personal data for RUSI researchers and subcontractors:

1. Whenever someone believes they will be processing personal data (information which relates to a living identifiable individual), they must have identified the lawful basis under which they will be carrying out the processing. Generally, RUSI researchers and subcontractors will use legitimate interest or consent as their lawful basis.

    i) Legitimate interest will be considered a lawful basis for processing personal data if it passes the purpose, necessity, and balancing tests (also known as a legitimate interest assessment or LIA). This in practice means you must have clearly identified the **purpose** for the processing and whether that processing is **necessary** to achieve the identified purpose. If you can achieve the same results without having to process personal data, then processing is not considered necessary and is therefore unlawful.

    After determining purpose and necessity, you will then have to **balance** your intended purpose vs the impact the data processing might have on the data subject's rights. If the impact on the data subject's rights is within reason, then you can process their personal data based on legitimate interest. If you determine processing is necessary but would unfairly impact the data subject's rights, then although the processing might be necessary it wouldn't be fair.

    Please bear in mind that as RUSI is a small organization, it is not required to document legitimate interest assessments. However, having proof to show the ICO that you've given enough thought to the reasons why you are choosing to collect and process personal data in your research would be advisable.

    ii) Consent will be considered a lawful basis for processing personal data when it is given by the data subject freely and in an informed manner. This means people can not be pressured or tricked into giving their consent. All relevant information in relation to the project and how their information is going to be used must be provided so people are aware of what they are agreeing to.

It's very important to bear in mind when choosing consent as a lawful basis for processing personal data, that consent can be withdrawn at any moment, meaning data subjects have full control over how their data is processed and for how long.

The ICO points out that when conducting research "in most cases, consent is not the most appropriate lawful basis[1]"as it can be withdrawn and may impact research results. This in practice means researchers will usually rely on legitimate interest. However, when processing special categories of personal data such as ethnic background, sexual orientation, union membership status[2], etc. **explicit consent** will be required which is where RUSIs interview consent forms may be used.

Consent as a lawful basis for the processing of personal data **must not be confused** with requesting consent from participants when conducting research, which is required from an ethical perspective.

2. Researchers and/or subcontractors may choose to anonymize personal data they have collected when conducting research as once personal data has been anonymized data protection legislation no longer applies to it[3].

3. By making sure there is a clear lawful basis for processing, researchers and subcontractors will be abiding by the first principle of data protection regulations which is: lawfulness, fairness, and transparency. However, they should also bear in mind:

   i) **Purpose limitation**: processing of personal data needs to relate to the purpose it was collected for.
   ii) **Data minimisation:** it's best to do as much as you can with as little information as possible. Avoid requesting and/or storing information which is not essential to your purpose.
   iii) **Accuracy:** personal data must be accurate and up to date.
   iv) **Storage Limitation:** data should not be kept longer than it is strictly required to fulfil the identified purpose.
   v) **Integrity and Confidentiality:** all personal data we process must be trustworthy and kept safe and confidential.

4. Specifically, to abide by the integrity and confidentiality principles, researchers and subcontractors must abide by RUSIs Cyber Security Policies. Other practical advice includes:

[1] https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/the-research-provisions/principles-and-grounds-for-processing/
[2] A full list of what data falls under a special category can be found at: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/special-category-data/what-is-special-category-data/#scd1.
[3] https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/the-research-provisions/principles-and-grounds-for-processing/

To ensure data integrity:

- Validate input data: always check that whatever information going on any record is accurate and useful.
- Implement access controls: tightly control who has access to personal data and limit file and information sharing.
- Always backup data: to ensure recovery is possible if there is a breach.

To ensure data confidentiality:

- Restrict access.
- Encrypt files.
- Have confidentiality agreements where necessary.
- If data must be disposed of, ensure it's done safely and effectively.

Further guidance can be found at the ICOs webpage but please feel free to contact RUSIs Risk and Compliance Manager at compliance@rusi.org if you have any questions.