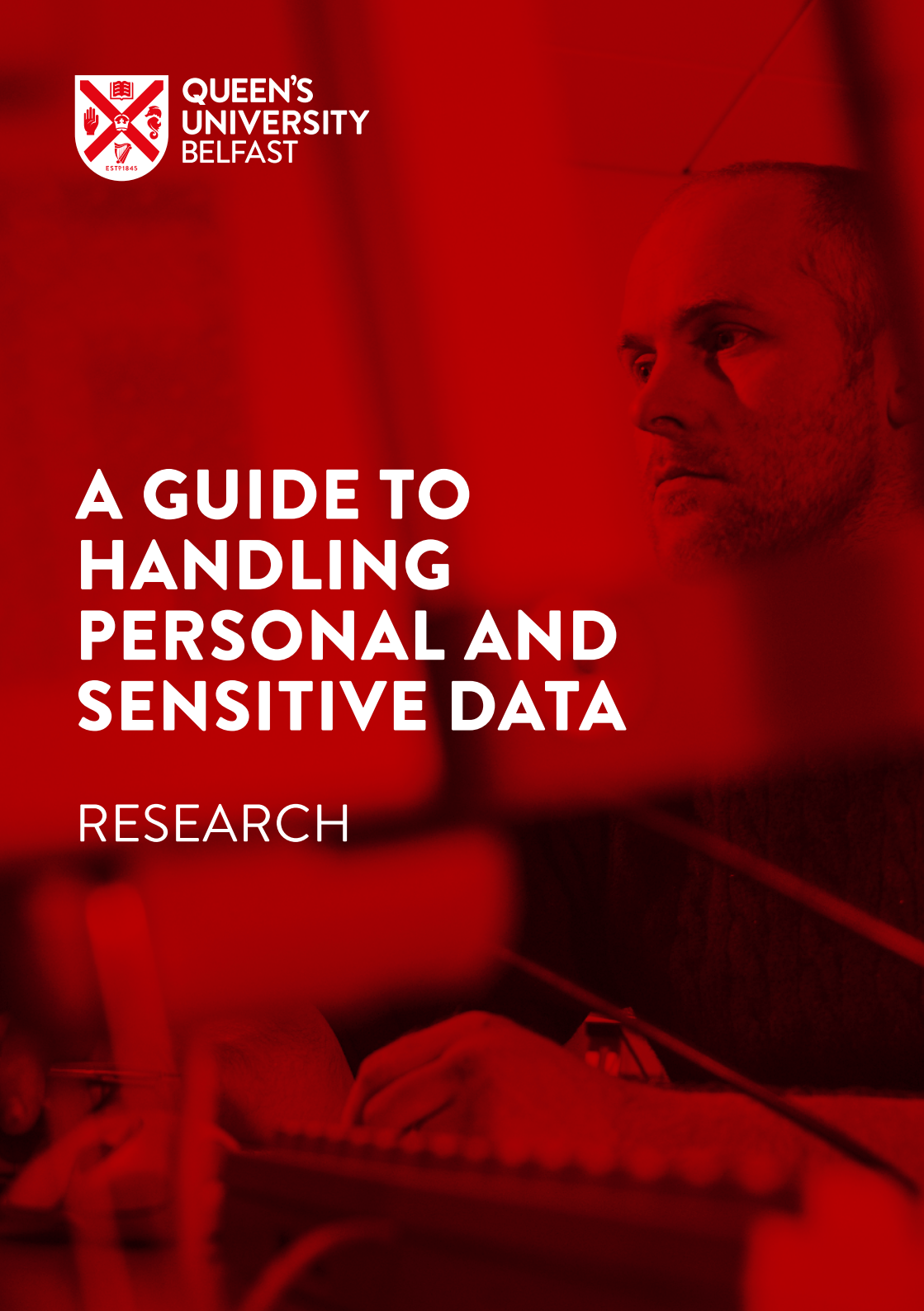
QUEEN'S UNIVERSITY BELFAST

ESTD1845

A GUIDE TO HANDLING PERSONAL AND SENSITIVE DATA

RESEARCH



Research

When conducting research which requires human participants and involves the collection, storage, processing and transfer of personal and/or sensitive data, we should ensure that data protection is considered **by design and default**. Completion of a **Data Privacy Impact Assessment (DPIA)** is a clear way to demonstrate that we are meeting this legislative requirement.

Not only will it help satisfy the data protection by design and default requirement it will support compliance with other GDPR principles, including **'Accountability'** and **'Data Minimisation'**. We are also required to ensure **'Transparency'** as part of GDPR. This means that we inform our data subjects of the data and processing taking place. Usually, this will take the form of a **Privacy Notice**.

Accountability

This GDPR principle was added so that data controllers won't just have to say they are compliant, they have to prove it. This is done with the appropriate documentation required, such as a DPIA or an Information Asset Register (IAR). If there are ever any issues and the supervisory authority for data protection in the UK (The Information Commissioners Officer – ICO) is required to investigate, they will ask for this documentation in order to ascertain what consideration and actions were taken in respect of the legislation and processing taking place.

Data Minimisation

This principle applies to how we collect data, or more importantly, what data we collect. It is important that we do not collect more data than we require for the purposes of the processing actions needed. For example, if we are conducting some research and we see that a data field is listed as date of birth (DOB), the question would be asked 'why do you need the DOB?' If the answer was 'to calculate age', then it could be identified that this data field could be 'minimised' or more accurately, the risk associated with this data field could be reduced, if it were changed to simply 'age' or 'age band'. More can be done with a DOB that can be done with someone's age. This would also apply to addresses and post codes. Ask the question, 'why do I need this?' and if it can be 'reduced/minimised' or removed completely, this would mitigate some of the residual risks.

Sharing

It is important to understand when and how sharing will take place as part of your research project. You should use the DPIA process to help map out these actual and potential transfers and any implications this may have. For example, transferring EU citizen data outside of the EEA is prohibited, unless there is an adequacy agreement with the country, they are part of the US Privacy Shield or there are adequate EU model clauses included in any contract or data sharing agreements (DSA). The use of DSA's is mandatory for any sharing of raw and pseudonymised personal and sensitive data between QUB and third parties. Templates are available on request from the ICU. When sharing data, we must ensure that any transfers are secure and done via appropriate mechanisms. For example, we would not want personal/sensitive data sent via email in an unsecure attachment. Sometimes, the use of DSA's are not required. This would generally be the case if there is a collaboration agreement or similar, which includes data protections clauses or appendixes.

Privacy Notices

A privacy notice (or a fair processing notice as they are also called) is how we communicate what we do with data subjects' personal and sensitive data. The privacy notice will inform individuals of how and where we collect their data, what we do with it, what our lawful basis or bases for processing are, how long it will be kept and with whom we are sharing it. These may be required for some projects but please liaise with the Information Compliance Unit for further advice as templates and guidance can be provided.

Anonymisation and Pseudonymisation

These words may seem to mean the same thing but they mean very different things when it comes to data protection. Firstly, if something is truly **anonymous**, the Data Protection Act 2018 **will not be engaged** and GDPR and DPA 2018 will not apply. However, this is rarely the case. More often than not, the data set will be **pseudonymised**. This means that, although some identifying information has been removed, such as removing a name and adding a unique identifier (ID or code), other information is still present which could be used with other data to identify the individual.

The only significant difference is that **pseudonymised data will be treated as identifiable**, i.e. it will be subject to the DPA 2018 and GDPR rules. This doesn't mean that identifiable data is suddenly off limits, rather, we must ensure it is protected during processing, transfer and storage.

In practical terms, we should still ensure that we attempt to protect all human participants by engaging in a process of pseudonymisation wherever possible. In some cases, fully identifiable data may be required. If this is the case, then the security of the data during storage, processing and transfer is paramount.

If you require any assistance with the data privacy implications of your research, please contact the Information Compliance Unit **info.compliance@qub.ac.uk**