NUFFIELD DEPARTMENT OF PRIMARY CARE HEALTH SCIENCES

Feb 2021 v 1.0

Update on "Privacy by Design" Research Requirements

The University "Privacy by Design" (PBD) **requirements** were established to help the Department meet the data protection principles and safeguards as they apply to the processing of data for new research studies, trials, etc.

The PBD review generally applies to Department projects which intend to process personal data (includes pseudononymised data sets) **and** for which the Department functions as a Data Controller under GDPR.

For a new project, the review is initiated by completing a screening assessment, which determines the extent to which the Department's planned processing of data for that project poses risk. The outcome dictates the next steps for the review as referenced on **page two** of this document, including whether the project involves the use of any product or service to process data (e.g. by an external third party and/or through an internally developed/hosted application).

- ✓ Effective ***15 February***, the Department **prohibits** the collection and processing of any data subject to this review **before** a PBD review is completed.

- ✓ Based on the range of time required to complete a PBD review (one to four months or longer), the Department recommends that the Information Asset Owner (IAO) or designee for a new project initiate this review **either** in anticipation of a funding award notice or immediately upon notice of a funding award (e.g. parallel to ethics approval, where applicable) so as to prevent any delays in processing.

For **existing** projects to which this review applies and which were initiated before this date:

- ✓ A PDB review does not need to be conducted retrospectively;

- ✓ However, if any of these projects change the way[s] in which data are processed, they are subject to this review, such as when an ethics amendment is required to approve the change[s];

- ✓ In addition, if any of these existing projects use a product or service to process data (e.g. by an external third party and/or through an internally developed/hosted application) **and** the University Information Security Team did not previously vet that product or service, please contact the IG Team (**datasecurity@phc.ox.ac.uk**) for assistance with completing this step.

A new, IG Policy on the PBD review process is being finalised and will be distributed soon.

In the meantime, please contact the IG Team with any questions. Thank you.

Refer to Next Page

Privacy By Design (PBD)

1) PBD review mandated by GDPR (May 2018)
2) Intended to assess risk with the data processing of any *new* Department study or trial (Project) **before*** it begins, including use of third party services or products.
3) PBD generally applies to any Project where the Department serves as the Data Controller/Sponsor **and** processes Personal Data (even if pseudomymised).
4) Review consists of an initial screening and further assessment based on screening outcome.

***Some bodies, such as funders and data registries, are requesting to see DPIAs for projects as a condition for obtaining funding/data, irrespective of whether projects meet the legal criteria of high risk processing.**

Step #1

Is a Project Subject to PBD Review?

Yes

No

Step 1a: Initiate InfoSec Review[s]

For use of any internal product or service, which will be used to process personal data, check whether it was vetted by InfoSec; if not, complete BCSA

For any external third party product or service, which will process personal data on the Department's behalf, complete TPSA review with InfoSec and secure required contract(s)

Step #2

Initial Screening
Complete screening on ICT template (**https://compliance.admin.ox.ac.uk/privacy-by-design**)
Email it with any questions to the IGM (datasecurity@phc.ox.ac.uk)

Screening Determines That Processing Poses Low Risk

Screening Determines that Processing Poses Med-High Risk

Step #3

Complete DPA

Initiate Step 1a: InfoSec Review

Complete DPIA

Obtain Feedback from ICT

Step #4

Finalise DPA with IGM, obtain SIRO sign off and retain PDB documents. Initiate new review if there is a change to how data is processed.

Finalise DPIA with IGM, obtain SIRO signoff and forward to University DPO (thru ICT) for final

Retain PDB documents. Initiate new review if there is a change to how data is processed.

Review Duration: 2-4 weeks

Review Duration: 2-4 Months