East London
NHS Foundation Trust

Data Protection by Design and Default

Version number :	1.0
Consultation Groups	All staff
Approved by (Sponsor Group)	Information Governance Steering Group
Ratified by:	Quality Committee
Date ratified:	17th June 2020
Name of originator/author:	Associate Director of Information Governance / Data Protection Officer
Executive Director lead :	Paul Calaminus
Implementation Date :	July 2020
Last Review Date	June 2020
Next Review date:	June 2023

Services	Applicable
Trustwide	x
Mental Health and LD	
Community Health Services	

Version Control Summary

Version	Date	Author	Status	Comment
V1.0 Final	05.03.2020	DPO	Draft	Circulated for consultation prior to submission at May 2020 IGSG

Contents

1.0 Introduction

The General Data Protection Regulation (GDPR) requires organisations to have appropriate technical and organisational measures to implement data protection principles and safeguard individual rights. This is called 'Data protection by design and default'.

Under GDPR this is a legal requirement. Article 25(1) specifies the requirements for data protection by design. Article 25(2) specifies the requirements for data protection by default.

'Data protection by design and default' includes data protection as a core aspect wherever there could be a potential impact on processing personal data. A Data Protection Impact Assessment (DPIA) is a mandatory tool in the 'Data protection by design' process.

2.0 Purpose

This policy sets out the Trust's approach to 'Data protection by design and default'.

Designing projects, processes, products or systems with data protection in mind is an essential tool in minimising privacy risks. The consideration of data protection by design and default at an early stage reduces the likelihood of data protection breaches, increases transparency and aids joined up working with partners.

A Data Protection Impact Assessment (DPIA) is used as a tool to determined data protection considerations. This is mandatory since the introduction of the General Data Protection Regulation, including the requirement to publish DPIAs. Organisations may be fined for failure to comply.

This policy sets out when a Data Protection Impact Assessment is required, together with the process to be followed.

3.0 Duties

Chief Executive – has overall responsibility for ensuring the personal data of individuals is processed in accordance with the law. This includes service users, staff, carers, complainants, volunteers and contractors.

Senior Information Risk Owner (SIRO) – is responsible for overseeing the risk management of information assets.

Information Asset Owners (IAOs) – are Service / Associate Directors with overall responsibility for a service or function and the information assets relevant to that service. They provide assurance that information assets and their associated risks are being managed effectively. IAOs are accountable to the SIRO.

Information Asset Administrators (IAAs) – are operational managers who routinely use and maintain information assets. They provide evidence of compliance. IAAs are accountable to IAOs.

Data Protection Officer (DPO) – ensures the Trust meets its data protection and confidentiality responsibilities under various legislation. The DPO scrutinises and makes decisions regarding data processing for all DPIAs.

Project Manager / DPIA proposer (referred to as the proposer) – is the individual who is assigned initial responsibility for a project, initiative, service acquisition or redesign, information sharing agreement or new / updated product where there could be an impact on the processing of personal information of individuals.

4.0 When to complete a Data Protection Impact Assessment

A DPIA should be considered whenever there is likely to be an impact on the processing of person identifiable information. The Trust's Data Protection Officer will advise, but a DPIA should be routinely completed for four overarching circumstances:

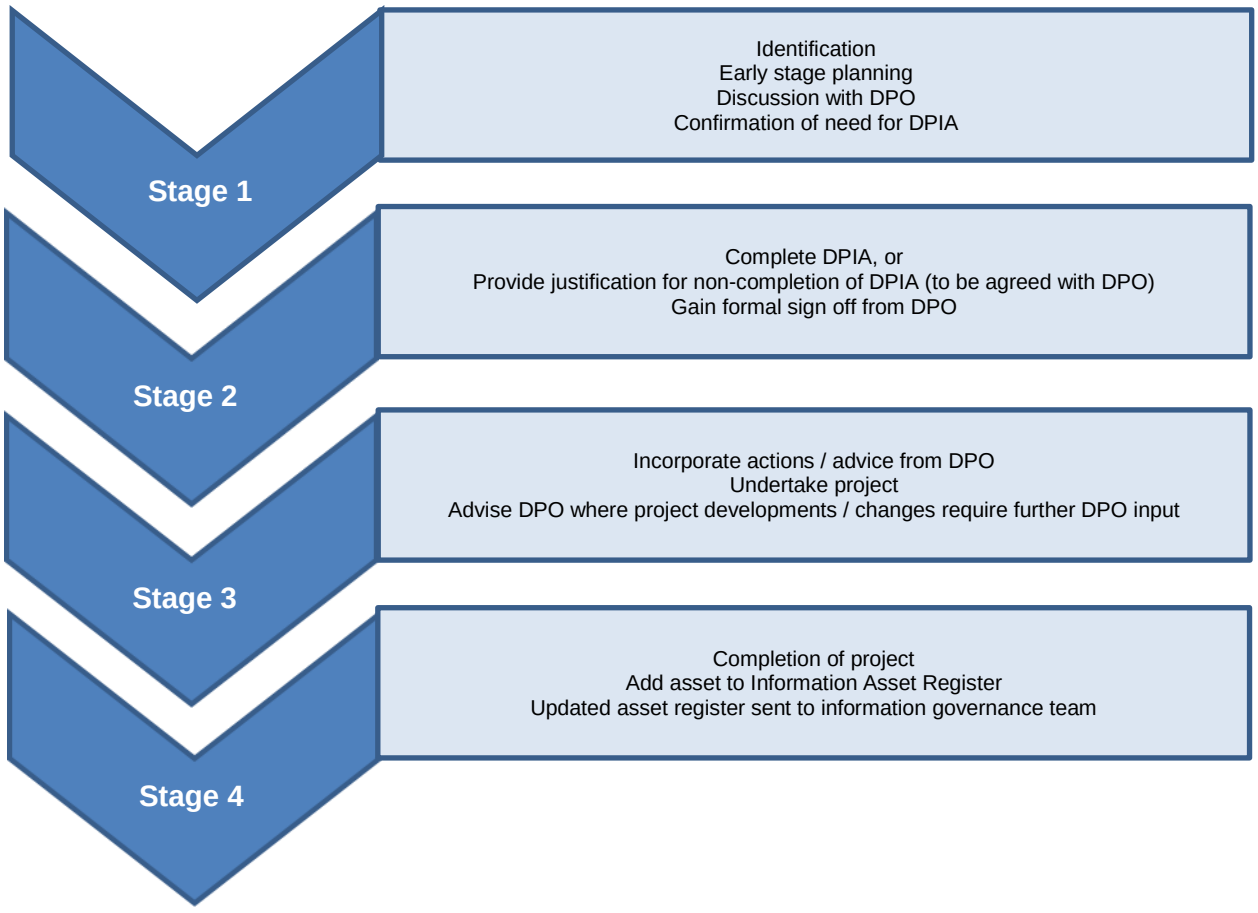
- New or significantly changed technology - where a new technology is being deployed e.g. building a new IT system for storing or accessing personal data, new software, new apps, health information exchange technologies etc.

- Profiling operation - where a profiling operation is likely to significantly affect individuals e.g. embarking on a data sharing initiative involving high intensity users for admission avoidance.

- Large scale processing - where processing on a large scale is likely to affect special categories of data e.g. business development, new or revised contracts, service acquisition or internal redesign / reconfiguration of services, information sharing, third party access to Trust systems containing person identifiable data.

- Divestment or decommissioning – of services and technology, where there is likely to be an effect on records containing person identifiable information, transfer of records, de-registration with the Information Commissioner's Office etc.

5.0 Stages



Stage 1

Whenever there is the potential for an initiative to affect the processing of person identifiable data there should be an initial discussion with the Trust's Data Protection Officer to outline:

- What the initiative is – contract, commissioning, new / changed technology, information sharing, service redesign, de-commissioning of services or software etc
- If there is likely to be an impact on an individual's rights and freedoms
- If the initiative will change the way data is collected, used and stored
- Timescales and partners involved

The Data Protection Officer (DPO) will advise if a Data Protection Impact Assessment (DPIA) should be completed. The information governance team will share the relevant documentation to be completed.

Stage 2

Completion of a Data Protection Impact Assessment (DPIA). The DPIA is a four part form:

- Step 1 – Project / proposal details
  - Project / proposal name
  - Description
  - Processing overview
  - Supplier involvement
  - Benefits
  - Implementation date

- Step 2 – Contact details
  - Work stream / project manager
  - Information Asset Owner (IAO)
  - Information Asset Administrator (IAA) / system owner
  - Executive sponsor

- Step 3 – Screening questions
  - Categories of data subject
  - New or additional information technology with a high impact
  - Data subject involvement
  - New information sharing
  - Using information in a new or different way
  - Intrusive technology
  - Research, planning, commissioning purposes
  - Changes to delivery of care
  - Intrusion
  - Other organisations
  - Consent
  - Significant changes to the way personal information is handled
  - New consolidation or linking of personal data
  - Cloud services
  - Children or vulnerable adults (service users)

- Step 4 – Full DPIA. Answering 'Yes' to any of the screening questions in Step 3 will result in the completion of a full DPIA

- Step 4.1 - Processing
  - What data will be collected / processed
  - How
  - Where from
  - Use
  - Manual / electronic processing
  - Access
  - Minimum data
  - Anonymisation / pseudonymisation
  - Third party access
  - Sending externally
  - Contract / data processor agreement
  - Retention, de-identification and destruction
  - Risks
  - Consultation processes

- Step 4.2 – Cloud considerations
    - Cloud provider base
    - Cloud hosting
    - Business continuity
    - Contract completion
    - Ownership
    - Policies

Once completed, the DPIA should be returned to elft.information.governance@nhs.net The information governance team will undertake an assessment according to the Principles contained in the Data Protection Act and in consultation with the DPO apply a risk assessment.

The DPO will make a decision regarding the proposal, according to data protection legislation, and advise the requester accordingly.

Stage 3

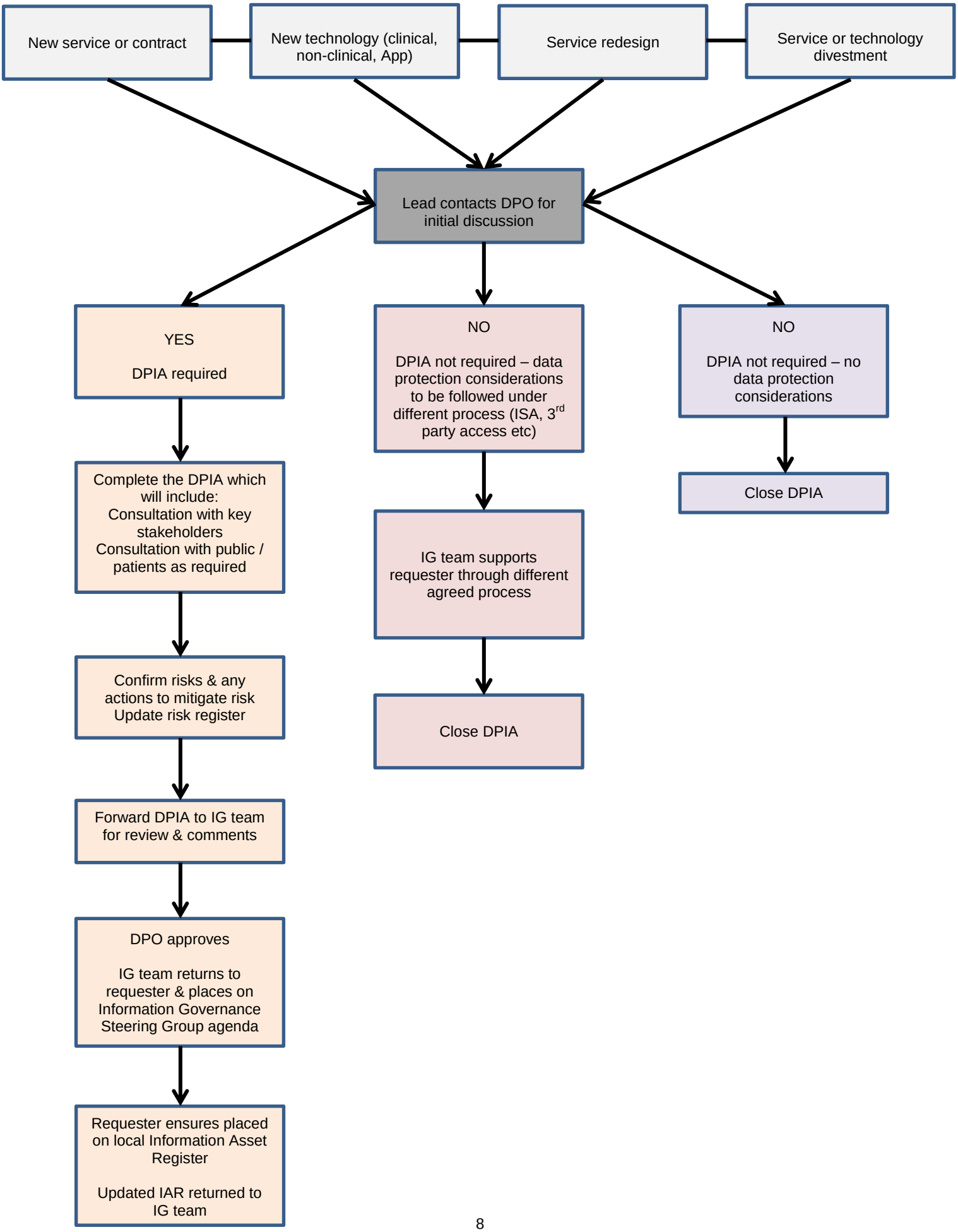
The proposer / project manager will undertake the project, liaising with the Data Protection Officer where new developments or changes to the original proposal emerge. Risks should be added to the relevant risk register and be escalated for inclusion in the corporate risk register where necessary.

Stage 4

On completion of the project the proposer must:

- Advise the Information Asset Owner of completion
- Add the asset to the Information Asset Register
- Send the update Information Asset Register to the information governance team on completion

6.0 Process


New service or contract
New technology (clinical, non-clinical, App)
Service redesign
Service or technology divestment
Lead contacts DPO for initial discussion
YES
DPIA required
NO
DPIA not required – data protection considerations to be followed under different process (ISA, 3rd party access etc)
NO
DPIA not required – no data protection considerations
Complete the DPIA which will include:
Consultation with key stakeholders
Consultation with public / patients as required
IG team supports requester through different agreed process
Close DPIA
Confirm risks & any actions to mitigate risk
Update risk register
Forward DPIA to IG team for review & comments
DPO approves
IG team returns to requester & places on Information Governance Steering Group agenda
Requester ensures placed on local Information Asset Register
Updated IAR returned to IG team

7.0 Who completes a Data Protection Impact Assessment?

Proposers of any new initiative that is likely to affect the way personal information is processed should alert the Data Protection Officer in the first instance. This includes potential acquisition and divestment of services, service redesign, contracts, new software, new ICT, information sharing, using technology or person identifiable information in a new way etc.

This means individuals in the Business Development Unit, Procurement and ICT should be particularly mindful of the need to consider data protection and confidentiality at an early stage. An initial discussion with the DPO will not necessarily always result in a request for completion of a DPIA.

A DPIA can be completed by anyone involved in the 'project'. This may be a project manager, subject matter expert or team manager and is dependent on the type of project. This individual is usually referred to as the 'proposer'. The proposer should attach as much information to the DPIA as possible to enable the information governance team to undertake an assessment without the need for requesting additional information.

High risk or large scale projects may be discussed at Trust meetings where appropriate (often Digital Board). Smaller projects or those with little risk will be approved by the DPO and taken to Information Governance Steering Group for information prior to a summary being published.

Although there is usually an assigned proposer of a DPIA, the DPO may seek input from other individuals or a wider team who have an understanding of the project's aims (including external partners), an understanding of the Trust's culture and priorities, have expertise in technology and technological processes, are able to assess and communicate organisational risk and are able to communicate effectively with stakeholders and management.

8.0 Ownership of data protection risk

Whilst the DPO will advise on data protection legislation, compliance and risk mitigation, ultimately the risk belongs to the service area concerned. This is in accordance with the principles of Information Asset Ownership. In ELFT, Information Asset Owners are Service or Associate Directors and own the risk for their functions. The DPO will liaise with the Senior Information Risk Owner (SIRO) where risks are identified, prior to approving a DPIA. Proposers must therefore assure themselves that all information and associated risks have been clearly identified and communicated during the DPIA process.

Similarly, any changes following approval of the DPIA must be notified to the DPO – for example, a small pilot that is later rolled out Trust-wide, an additional use of Office 365 to the original proposal, adding new partners to an existing information sharing agreement etc. Changes will be considered on a case by case basis but may result in a new DPIA.

Endorsement of a proposal through the DPIA process may be time limited – for example, an electronic means of communicating with patients may be approved during a pandemic to reduce clinical risk but may not be approved for long term use.

9.0 Proposal implementation

Once a proposal has been approved and implemented (becomes business as usual), the asset must be added to the relevant local information asset register and any associated data flows mapped.

The updated information asset register must be sent to the information governance team to be held as part of the centralised information asset register.

The information governance team will ensure, where appropriate, that the asset is added to the published Record of Processing Activity. This is a mandatory requirement under the General Data Protection Regulation.

It is important that during a procurement processes, tender evaluation questionnaires contain sufficient pass / fail questions relating to data protection and that any eventual contracts contain mandatory data protection clauses and data processing agreements. The Business Development Unit / Procurement team should hold a separate register of contracts.