NHS
Counter Fraud Authority

Data Protection by Design and Default Guidance

October 2019

FCG-IG-CP-014: Version: 2.0

NHS fraud.
Spot it. Report it.
Together we stop it.

Version control

Version	Name	Date	Comment
V.1.3	Finance & Corporate Governance	March 2019	Draft
V.2.0	Finance & Corporate Governance	October 2019	Annual Review October 2020

Table of contents

1. Introduction 4
2. What is privacy by design? 5
3. High risk processing 6
4. What is a DPIA under GDPR? 7
5. Associated GDPR provisions 8
6. Is the process the same under GDPR? 8
7. Ownership of Data Protection Risks 8
8. Throughout the project 8

1. Introduction

1.1 This guidance and procedure document sets out how the NHS Counter Fraud Authority (NHSCFA) will embed a culture of privacy by design in the way it conducts its business. Whenever a piece of work starts which involves using information about individuals (their personal data) we will look at the risks that may be associated with it. We will always make sure that the data protection core principles are met.

1.2 For matters, which if not properly addressed, might involve a serious risk to privacy, NHSCFA will carry out a Data Protection Impact Assessment (DPIA).

1.3 It has always been good practice to adopt a 'privacy by design' approach and to carry out a Privacy Impact Assessment (PIA). However, the General Data Protection Regulation (GDPR) makes privacy by design an express legal requirement, under the term 'data protection by design and by default'. It now makes DPIAs mandatory in certain circumstances.

1.4 As early as possible in any project or proposal, the officer responsible for the planned project will need to complete the organisation's DPIA form which is based on the Information Commissioner's Office (ICO), recommended template.

1.5 There is no need to delay the completion of a DPIA form if initial plans are not fully developed, as the process is particularly useful if it can inform projects at an early stage, as plans may be delayed or halted completely if data protection considerations are not fully risk assessed and sign-off obtained.

1.6 This guidance applies to staff responsible for the delivery or management of a project or business process (see PAAID & checklist documents), or the management of a contract or similar arrangement where the proposed activity will involve the processing of personal data.

1.7 It will apply where new technology is being introduced, which will include any proposed purchase of hardware, software, third party or cloud hosted services and proposals which involve the processing of personal data on databases, websites, mobiles and other Apps'[1].

1.8 Under data protection legislation the NHSCFA has an obligation to make thinking about how it protects personal data, an integral part of the way in which it conducts its business. How personal information will be looked after needs to be considered at the start of a process; developed along with the project and then monitored once it transfers to business as usual.

[1] See Redmine IT Business Case Request process.

1.9 The aim of this guidance is to identify and minimise privacy risks while still meeting required business aims. Ideally it should be applied before procurement activity starts, irrespective of value of the procurement, including proposals with nil cost.

2. What is 'privacy by design'?

2.1 Privacy by design is an approach to projects that promotes privacy and data protection compliance from the start. Previously, these considerations were often bolted on as an after-thought or ignored altogether.

2.2 Privacy by design describes the meaning of data quality, who is responsible for its maintenance and how continued improvements can be made.

2.3 The ICO encourages organisations to ensure that privacy and data protection is a key consideration in the early stages of any project and then throughout its lifecycle. For example when:

- building new IT systems for storing or accessing personal data;
- developing legislation, policy or strategies that have privacy implications;
- embarking on a data sharing initiative; or
- using data for new purposes.

2.4 The ICO wants to see more organisations integrating core privacy considerations into existing project and risk management methodologies and policies. All NHS organisations are required to have DPIAs in place in order to comply with the current Data Security and Protection Toolkit.

2.5 A DPIA is required in situations where data processing is likely to result in high risk to individuals (see further below). Cost is not a factor - the relevant consideration is whether a proposal involves the processing of personal data. If personal data is to be used to any extent, the proper use and safeguarding of that data needs to be considered. **Therefore within NHSCFA, any project that involves the use of personal data will require the completion of DPIA.**

2.6 Where a DPIA indicates that the data processing is 'high risk' and we cannot sufficiently address those risks, we will be required to consult the ICO to seek its opinion as to whether the processing operation complies with GDPR. Staff will need to start assessing situations necessary to conduct a DPIA. Consideration will need to be given to:

- who will conduct it?
- who else needs to be involved?

- will the process be undertaken within the business unit or centrally for wider input?

3. High risk processing

3.1 Proposers of high risk projects will need to complete a DPIA form along with the necessary PAAID document. This will provide for a more in depth look at the application of data protection and cyber security requirements, the associated risks and how they may be mitigated. It will be important to demonstrate that high risk processing has had sufficient safeguards applied to minimise any risk. Failure to do so could result in the Information Governance Lead/Data Protection Officer (DPO), Senior Management Team (SMT) or ultimately the Information Commissioner vetoing the processing.

3.2 High risk processing is likely to arise where there is a significant change in the way in which personal information is used. This is likely to be where:

- the project or proposal has a wide scope
- it uses new or intrusive technologies
- particularly sensitive or high risk data or individuals are involved
- information was collected for one purpose but is now intended to be used for another.

3.3 This is likely to apply where the proposer is:

- implementing a new or unusual type of technology
- using special category (sensitive) personal data, or the scope of personal data increases
- consolidating information held by different parts of the organisation
- using personal data already held for a new purpose
- sharing personal data, pooling or linking data with other organisations.

3.4 Successful completion of the DPIA will involve those familiar with the proposed project or a team with a range of expertise and skills. Important features will include:

- an understanding of the project's aims and the organisation's business functions

- authority to influence the design and development of the project and participate in decisions
- expertise in privacy and compliance matters
- expertise in technology, processes and activities relevant to the project;
- ability to assess and communicate organisational risks
- ability to assess which privacy solutions are feasible for the relevant project.

3.5 Whilst DPIA's are usually reserved for high risk proposals, **they must be completed for all NHSCFA projects that involve the processing of personal data** and therefore it is essential that sufficient time is allowed for proper consideration to take place. The proposal may not become operational until any identified data protection issues have been resolved or satisfactorily mitigated.

3.6 Data protection legislation requires the advice of the DPO to be sought when carrying out a DPIA. Once data protection risks have been managed to the satisfaction of the DPO, it can be signed off.

3.7 Staff involved in such projects should familiarise themselves with the guidance the ICO has produced on DPIAs[2] and on how these are to be implemented. The guidance also shows how DPIAs can link to other organisational processes such as risk and project management. Additional information and guidance on how to complete the form can also be sought from the Information Governance team.

4. What is a DPIA under GDPR?

4.1 Article 35 of GDPR defines DPIA as:

Where a type of processing in particular using new technologies and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks[3].

[2]https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias-1-0.pdf
[3]Recital: 75, 84, 89

5. Associated GDPR provisions

5.1 The relevant GDPR Articles that relate to DPIA's are 35, 36 & 83 as well as the following accompanying Recitals 84, 89-96.

5.2 What's new?

ICO's Data Protection definition:	GDPR definition:
Privacy impact assessments (PIAs) are a tool which can help organisations identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy. PIAs are an integral part of taking a privacy by design approach.	The GDPR makes privacy by design an express legal requirement, under the term 'data protection by design and by default'. It also makes 'Data Protection Impact Assessments' (DPIAs) mandatory in certain circumstances.

6. Is the process the same under GDPR?

6.1 The process remains the same, however:

- a new ICO recommended DPIA template requires completion; and
- there is a need to ensure governance processes for sign off are robust.

7. Ownership of Data Protection risks

7.1 While the DPO will advise on data protection legislation, compliance and risk mitigation, ultimately the 'risk' belongs to the business unit concerned. The Leadership Team (LT) Lead must satisfy themselves that they have sufficiently identified and considered the project risks in relation to data protection.

8. Throughout the project

8.1 It is unlikely that all of the required information will be to hand at the outset of a project or proposal. It is therefore particularly important during any procurement process that tender evaluation questionnaires contain sufficient pass/fail questions relating to data protection and that any eventual contracts contain the mandatory data protection clauses and description of data processing.