General Dental Council

Data Protection Impact Assessment Policy

Owner	Information Governance
Author	Information Governance Manager
Reviewed by	Principal Legal Adviser
Approved by and date	EMT 6 September 2016
Effective from	January 2017
Review Date	November 2020 (reviewed every year)

Version History

Date of next revision: November 2021

Revision Date	Previous Revision Date	Summary of Changes	Changes Marked
25/10/2019		Updated to include changes post GDPR and requirements for Data Protection Impact Assessments	
18/11/2020		Minor amendments and full list of special category data types included in screening Question 1	

1. Policy Statement

1.1 The GDC is committed to ensuring it appropriately manages and protects personal data. The Data Protection Impact Assessment (DPIA) Policy is part of the GDC's information governance policy framework and helps ensure privacy and information security risks are considered at the outset of projects and incorporated into the planning and risk management process.

2. Definitions

2.1 DPIA is a process designed by the Information Commissioner's Office to help organisations analyse, identify and mitigate against all data protection risks from a project or planned change in the way we process personal data.

3. Purpose

3.1 The aim of a DPIA and of this policy is to help the GDC identify the most effective way to comply with its data protection obligations, ensuring that expectations of privacy and risks to personal data are considered and mitigated at the outset or early stage of a project and are regularly reviewed and updated as the project progresses.

3.2 DPIAs help reduce the risk of the organisation failing to meet its obligations under the General Data Protection Regulation (GDPR) and Data Protection Act 2018 as well as helping to promote a data security conscious culture.

3.3 Under Article 35 of the GDPR, DPIAs are mandatory for organisations who process large volumes of personal data.

3.4 DPIAs provide the opportunity to identify and fix problems at an early stage. Publishing large DPIAs show transparency and enable individuals to see how and why we are processing their data.

4. Scope

4.1 GDC staff are required to formally consider the need for a DPIA as soon as it becomes clear that a project or significant process change involves the use, transfer, or storage of personal data. The Information Governance (IG) Team should be contacted and will assist with the process and completion of the documents. Guidance about how to complete a DPIA is provided in Annex 1.

4.2 The DPIA Screening Questions (Annex 2) should be answered at the outset. They indicate whether a DPIA is needed. Once the screening questions are completed and signed, they will be saved by the project manager together with the project documents and by the IG Team. Answering 'yes' to any of the screening questions is an indication that a DPIA is required and the DPIA template at Annex 3 should then also be completed and saved. Again, the IG Team and Project Manager will work together to complete this work.

4.3 As completed DPIAs identify information risks and how they will be mitigated, they should be formally signed and agreed by the project owner, or, if they are different, the information asset owner for the area of the business. Projects with a high risk should also have the DPIA agreed by the GDC's SIRO (Senior Information

Risk Owner). A copy of the DPIA will be saved as part of the project documents and by the IG Team.

4.4 The GDC will publish DPIAs for significant projects on its external website as part of its publication scheme.

5. Review and approval

5.1 This policy will be reviewed by the Information Governance Manager on an annual basis. The date of the next review will be November 2021.

5.2 The Information Governance Manager will consider and approve any minor changes or amendments without the need to seek fresh approval from the Executive Management Team.

5.3 Major amendments will be referred to the Information Governance Group and the Executive Management Team for fresh approval of the policy.

6. Related policies

6.1 Information Governance Policy

7. Annexes

1) Guidance
2) Privacy Impact Assessment Screening Questions
3) Privacy Impact Assessment template

Annex 1

Data Protection Impact Assessment Guidance

When is a DPIA likely to be needed?

Not every project will require a DPIA. DPIAs will usually be required when we intend to do something new or different with the personal data that we hold or collect. That could be the introduction of a new system or technology that stores and processes personal data. For example, recording the calls we receive on our customer advice and information line or introducing CCTV cameras to the floors in our offices. DPIA's are also likely to be appropriate where processing carries a high risk such as sensitive information.

DPIAs work best if they are considered and completed at the outset of a project (or as soon as it becomes clear that a project will impact on data privacy) when any issues it identifies can be incorporated into the project plan and risk management process.

This does not mean that a formal DPIA must necessarily be started and finished before a project can progress further. A DPIA can run alongside and evolve with the project development process or as the focus of the project changes and develops. This means it can be reviewed and updated with the project plan and risk assessment. What begins as a more informal early consideration of privacy issues can be developed into part of the DPIA.

Importantly, the time and resources dedicated to a DPIA should be proportionate and scalable to the project or changes being implemented.

Deciding whether a DPIA is needed

To help decide whether a DPIA is required, project managers should work with the IG Team to complete the DPIA Assessment Screening Questions at Annex A. A copy of the completed assessment questions should be retained by the project manager and the IG Team.

Answering 'yes' to any of the screening questions is an indication that a DPIA is required. However, the screening questions are not meant to be exhaustive and if you have any concerns regarding the changes the project will introduce and the potential for the project or changes to impact on the personal data held by the GDC, then a DPIA should be completed.

Completing a DPIA

Where a DPIA is necessary based on the assessment questions, the data protection assessment, consultation record, risk assessment, and sign off in Annex 3 should be completed with the involvement and assistance of the Information Team.

These are templates and depending on the project and its focus, the DPIA questions can and should be added to and/or amended. Large scale projects with a high degree of risk which have the potential to impact not just on the GDC but its stakeholders will naturally require a more detailed DPIA framed with narrative about the project its aims, risks, and mitigations.

DPIA questions and data law check

The DPIA questions help to scope the areas of risk and possible solutions.

The data protection check also helps scope areas of risk but is designed to more explicitly review and ensure data law compliance. It includes a data law check and a human rights assessment.

Consultation with internal and external stakeholders/partners

Though consultation will most obviously be required where the project involves multiple third party organisations, we are just as likely to need to consult and discuss proposed changes internally with the teams or business areas affected by the changes or implementation of new systems or processes.

The primary aim of the consultation is to draw out any privacy issues and risks that the DPIA and project will need to address and engage the stakeholders in helping to design the solutions. This is especially important where the stakeholders will be responsible for implementing the project or change of new systems and processes.

DPIA risk assessment

The risk assessment will incorporate but not be limited to issues identified in completing the DPIA questions and the DPA check. It will include risks to individuals, corporate risks, and compliance risks. These may include:

Risks to individuals

- Inadequate disclosure controls which increase the likelihood of information being shared inappropriately.
- The context in which information is used or disclosed can change over time, leading to it being used for different purposes without people's knowledge.
- New surveillance methods may be an unjustified intrusion on their privacy.
- Measures taken against individuals as a result of collecting information about them might be seen as intrusive.
- The sharing and merging of datasets can allow organisations to collect a much wider set of information than individuals might expect.
- Identifiers might be collected and linked which prevent people from using a service anonymously.
- Vulnerable people may be particularly concerned about the risks of identification or the disclosure of information.
- Collecting information and linking identifiers might mean that an organisation is no longer using information which is safely anonymised.
- Information which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, presents a greater security risk.
- Implementation difficulties cause restriction to loss of personal data or access to personal data.
- If a retention period is not established information might be used for longer than necessary.

Corporate risks

- Non-compliance with the DPA or other legislation can lead to sanctions, fines and reputational damage.
- Problems which are only identified after the project has launched are more likely to require expensive fixes.
- The use of biometric information or potentially intrusive tracking technologies may cause increased concern and cause people to avoid engaging with the organisation.
- Information which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, is less useful to the business.
- Public distrust about how information is used can damage an organisation's reputation and lead to loss of business.
- Data losses which damage individuals could lead to claims for compensation.

Compliance risks

- Non-compliance with the Privacy and Electronic Communications Regulations

(PECR).
- Non-compliance with sector specific legislation or standards.
- Non-compliance with human rights legislation.
- Non-compliance with the GDPR and DPA 2018.

There are many different steps which organisations can take to reduce a privacy risk. Some of the more likely measures include:

- Deciding not to collect or store particular types of information.
- Devising retention periods which only keep information for as long as necessary and planning secure destruction of information when no longer required.
- Implementing appropriate technological security measures.
- Ensuring that staff are properly trained and are aware of potential privacy risks.
- Developing ways to safely anonymise the information when it is possible to do so.
- Producing guidance for staff on how to use new systems and how to share data, if appropriate.
- Using systems which allow individuals to access their information more easily and make it simpler to respond to subject access requests.
- Taking steps to ensure that individuals are fully aware of how their information is used and can contact the organisation for assistance if necessary.
- Selecting data processors who will provide a greater degree of security and ensuring that agreements are in place to protect the information which is processed on an organisation's behalf.
- Producing data sharing agreements which make clear what information will be shared, how it will be shared and who it will be shared with.

DPIA sign off

DPIAs identify data privacy risks and solutions so it is important that once these are identified and agreed, as part of the DPIA process, that they are then incorporated and reflected in the project and risk management plans.

The risks and the identified treatments should be formally signed and agreed by the project owner, or, if they are different, the information asset owner for the area of the business.

A copy of the completed DPIA will be retained as part of the project documents and also by the IG Team.

Annex 2

Data Protection Impact Assessment Screening Questions			
Contact name and job title			
Description of New project, system, technology or legislation name being assessed			
Purpose/Objectives of the initiative (if statutory, provide citation)			
	DPIA Question	**Answer and details**	**Proposed mitigations/recommendations**
1	Will the project process special-category data (**race; ethnic origin; political views; religion; trade union membership; genetics; health; sex life; sexual orientation or biometrics)** or criminal-offence data on a large scale?		
2	Will the project involve a change to the nature, context purpose or scope of our existing personal data processing?		
3	Will the project process personal data that could result in a risk of physical harm in the event of a		

	DSI?		
4	Will the project use innovative technology in combination with any of the criteria in the European guidelines?		
5	Does the project carry out profiling on a large scale, use automated decision making for special category data or make significant decisions about people, including access to a service opportunity or benefit?		
6	Does the project combine, compare or match data from multiple sources?		
7	Does the project process personal data without providing a privacy notice directly to the individual in combination with any of the criteria in the European guidelines?		
8	Will the project process biometric or genetic data in combination with any of the criteria in the European guidelines?		
9	Does the project process personal data in a way that involves tracking individuals' online or offline location or behavior, in combination with any of the criteria in the European guidelines?		

10	Will the project process children's personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them?		
11	Will the project systematically monitor a publicly accessible place on a large scale?		

Need for DPIA identified? If yes, then explain reasons (refer to screening questions above). If a DPIA is not to be carried out the reasons should be documented. Please note, consideration for a DPIA should still be given even if none of the above questions are answered 'Yes'.

Completed by:

Signed:

Date:

Annex 3

Data Protection Impact Assessment

Contact name and job title	
Description of New project, system, technology or legislation name being assessed	
Purpose/Objectives of the initiative (if statutory, provide citation)	

1. Why do we need a DPIA?

What are the overall objectives of the project and what type of processing does it involve? Consider including a link to the business case

2. Describe the processing

What is the nature of the processing

How will the GDC collect, store and delete the data? Who will the GDC be sharing data with? Are there sufficient agreements in place? Does the project involve new or inherently privacy-invasive technologies? Does the project involve new or substantially changed identity authentication requirements that may be intrusive or onerous? Which of the processes are high risk? Consider including flow diagrams or links to any data mapping.

What is the scope of the processing?

What is the type of data? Is it special category data (race; ethnic origin; political views; religion; trade union membership; genetics; health; sex life; sexual orientation or biometrics (if used for ID purposes)). Does the project involve an additional use of an existing identifier for single or multiple purposes? What are the volumes of data being collected? How many individuals will it affect? What is the retention of the information? Will the project result in the handling of a significant amount of new data about each person or significant change in existing data holdings?

What is the context of the processing?
What is the relationship between the GDC and the data subjects? What control will the data subjects have and do they include vulnerable groups and children? Are there any security flaws and what are the technological capabilities in this area? Are there any concerns that the GDC should consider? Are any certifications required or codes of conduct?

What are the purposes of the processing?
What do we want to achieve from the processing? What benefits will it deliver and who will receive these benefits?

3. Consultation process

How will we consult with stakeholders?
When and how will we seek the views of individuals? Will it be through newsletters or more formal consultation and involve end users or processors? Will we require expert advice on any areas such as IT? If we decide not to consult what reasons do we have?

4. Necessity and proportionality assessment

What are the measures of proportionality and compliance?

What are our lawful basis of process and does it achieve our goals? Is the justification for the new data handling unclear or unpublished? Are there better or more secure ways we can do this? Is it futureproof and what are we doing to avoid function creep (a process where the purpose for the use of personal data gradually widens or is blurred)? How will we approach data minimization and data quality? What information will we be sharing with individuals?

5. Data security

Assess the levels of security of the project

How will we ensure personal data will be stored and processed securely? Will this require additional security measures? Will we require external advice? How will we ensure processors are compliant? What steps will we need to take in the event data is transferred between systems or internationally?

6. Risk assessment

Describe the source of the risk and potential impact on individuals. Include mitigation measures where the risk identified is medium or higher. In the event a high risk cannot be mitigated adequately, it may be necessary to consult with the ICO.

	Risk and impact on individuals	Likelihood	Severity	Overall risk	Mitigation options	Effect on risk	Residual risk	Approved?
1.								**Yes/No**
2.								**Yes/No**
3.								**Yes/No**
4.								**Yes/No**
5.								**Yes/No**

7. Sign off

Item	**Name/position/date**	**Notes**
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:		If we are accepting any residual high risk then we should consult the ICO before continuing
DPO advice provided		DPO should advise on compliance, mitigations and whether processing should proceed
Summary of DPO advice		

DPO advice accepted or overruled by:		If overruled, please explain your reasons
Comments:		
Consultation responses reviewed by:		In the event the decision differs from respondents we should explain our reasons
Comments:		

This DPIA will be kept under review by:		The DPO should also review ongoing compliance with the DPIA

Data Protection Act Compliance Check			
		Details	Action required
1	***Principle (a) – Lawfulness, fairness and transparency*** ***Personal data shall be processed fairly, lawfully and, in a transparent manner in relation to the data subject processed unless: a) at least one of the conditions in Schedule 2 is met, and b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.***		
		Details	Action required
1.1	Have you identified specific grounds for processing (these should follow the six bases for processing data). If no lawful basis applies, then this principle will be breached.		
1.2	Does this project involve handling of special category data? If yes, then this will require one of the 10 lawful bases of processing special category data. Please list the categories and the lawful basis of process.		

1.3	Does the processing result in other unlawful activities (such as copyright Human Rights Act 1998 etc.)?		
1.4	Will we be processing personal data in a way in which the subjects would expect?		
1.5	How will we inform the data subjects of the processing of their data? (This could be through our privacy statement or if applicable when we obtain consent)		
1.6	If you are relying on consent to process personal data, how will this be collected and what will you do if it is withheld or withdrawn?		

1.7	Do you need to amend your privacy notices? If yes, please describe how.		
2	***Principle (b) - Purpose limitation*** ***Data should be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.***		
2.1	Does the project involve the use of existing personal data for new purposes?		
2.2	How is the use of existing personal data for new purposes being communicated to (a) the data subject; (b) the person responsible for Notification within the GDC (c) the information commissioner		

2.3	Are the new purposes compatible with the original intentions?		
2.4	Are these new purposes fair, lawful and transparent in accordance with Principle (a)?		
3	***Principle (c) - Data minimisation*** ***Data collected should be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.***		
3.1	Is the personal data sufficient to serve its intended purpose/ good enough for the purposes it is used?		
3.2	What personal data could you not use, without compromising the needs of the project?		

4	***Principle (d) – Accuracy*** ***Personal data should be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.***		
4.1	How are you ensuring that personal data obtained from individuals or other organisations are accurate?		
4.2	What steps will we be taking to delete or correct inaccurate personal data?		
4.3	Will we need to carry out regular checks or updates to ensure data is accurate?		

4.4	Will we need to include a procedure in the event of a challenge to the accuracy of the data?		
5	***Principle (e)*** - ***Storage limitation*** ***Personal data should be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.***		
5.1	What retention periods are suitable for the personal data you will be processing? If being used and shared with third party partners, how long will they retain the information for?		
5.2	Will we need to review the retention periods and will this project cause any issues with our existing retention periods?		

6	***Principle (f) - Integrity and confidentiality*** ***Personal data should be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.***		
6.1	Do we have appropriate security measures in place to protect the personal data we hold?		
6.2	Are any risks suitably accounted for? Do we need to consider mitigation measures?		
7	***Accountability*** ***The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (fair, lawful and transparent).***		
7.1	Will we have sufficient policies and procedures in place when the project is implemented?		

7.2	Will staff need additional training?		
7.3	Will we need to undertake regular checks to ensure the outcome of the project remains fit for purpose?		
Conclusions			