Data Protection Impact Assessments

Tim Turner

Version 2: December 2020

Contents

1 What is a Data Protection Impact Assessment?

A Data Protection Impact Assessment (DPIA) is a process for ensuring that when a new initiative or substantial change to existing practice is underway, the implications for individual rights and the proper handling of personal data are properly considered. Rather than trying to bolt on solutions to problems later on (or having to live with problems you cannot solve), the aim of the DPIA is to ask questions while the project is still in the design phase. DPIAs, an evolution of what were known as Privacy Impact Assessments or PIAs, have been part of the landscape for many years and across many jurisdictions. The General Data Protection Regulation (GDPR) makes them mandatory in the UK for the first time.

DPIAs are not mandatory for all new processing, only those that represent a high risk to the rights and freedoms of the data subject, but it is worth bearing in mind that the process will be useful in many situations. Carrying out more DPIAs than you need to will likely result a greater awareness of risks and the opportunity to do something about them.

During the DPIA, you may identify a risk that is unacceptable, and which must be addressed in order to prevent a risk to individuals' privacy or interests, or to avoid breaching the law. Those carrying out the DPIA must be willing to alter features of their project if the risk is sufficiently significant or the consequences are sufficiently likely to come about. It is unlikely that the risks will be sufficiently great that the project will have to be altered radically, or (in an extreme case) abandoned – the purpose of the DPIA is to ensure that the project comes to fruition while dealing with the risks – but those more extreme outcomes are a possibility. There is even a slim chance of having to consult the Information Commissioner before continuing.

Being able to say that a DPIA was carried out may reassure stakeholders and service users in the abstract, but after implementation, if things go wrong that clearly could have been prevented in the design phase of your project, the existence of a glossy DPIA report will not help you. The DPIA is a process intended to reduce risk and make compliance more likely – it is not a tick box exercise that needs to be overcome and then forgotten about. It is a strand that starts as early as possible and ends when the project is complete or when the design of the project is fixed and will not change.

Two things are vital:

- You must be willing to contemplate how your project might go wrong,

cause harm or damage to people or how it and the data processed to make it work could be misused or exploited by others

- You must be willing to change the design of your project if the DPIA suggests that there is a risk that cannot be properly mitigated or prevented, especially if that risk is significant in terms of impact and likelihood

The objective of a DPIA is often perceived to be one of legal compliance, and it is true that the GDPR makes a DPIA mandatory in certain circumstances. There is an also a practical benefit: one of the biggest problems that Data Protection practitioners encounter is finding risks or breaches after a project has been launched, that have been made part of the design, at a point where they are difficult to mitigate. Those designing the project should also recognise that poor handling of personal data, or the incidents and bad headlines that can result, will have adverse effects on the project's success and the business overall. The attempt to manage privacy and data protection risks as part of the project design does not just protect the people who might be affected by the project and help comply with the law – it might well prevent the project from being delayed or halted by DP problems down the line.

2 Set-up

2.1 How does it work?

Several years ago, the UK Information Commissioner issued a Code of Practice on Privacy Impact Assessments that set out a framework for running a DPIA, breaking the process down into five steps, basing their approach on practice that was already well-established in other countries. The 2016 General Protection Regulation, which came into force in May 2018, codifies a very similar approach is based on the same practices. If you have adopted procedures based on the ICO's code, you should be close to operating a compliant and beneficial model of how to tackle a DPIA (indeed the European Data Protection Board's guidance on DPIAs identifies the ICO's old Code of Practice on PIAs as a model of good practice).

The GDPR describes the subject matter of the DPIA as a 'processing activity', but throughout this guide, like the ICO, I have used the word 'project'.

The stages of a DPIA in Article 35 of the GDPR are as follows

- Identify the need for a DPIA
- Create a systematic description of the project
- Assess whether the project is necessary and proportionate, including an assessment of whether the project is lawful
- Identify the risks to data subjects' rights and freedoms that the project represents
- Identify possible treatments for these risks and decide whether to implement them, balancing how great the risk is and the effect on the project
- Consult those people who are affected by the project and seek their views on the risks and their mitigation (this is optional)
- Record the risk decisions and make any necessary changes to the project plan

2.2 When do we carry one out?

Any new processing that started after May 25th, 2018 might be in scope, but the GDPR does not requires that every new project requires a DPIA. To avoid problems from the regulator, it is important to identify any project that meets the criteria for a mandatory DPIA.

If processing breaches the DPIA in future, and a DPIA should have been carried out but was not, it is likely to either provoke enforcement action, or exacerbate any penalty. It is unlikely that the ICO would ever be willing to take action solely because a DPIA was not carried out when it should have been, in the absence of any other issues. Nevertheless, if you see a DPIA as nothing more than a legal requirement, you are missing a huge opportunity. Think of a DPIA as an opportunity to assess risks and iron out problems at the most convenient point; be open to the possibility of carrying them out regularly, even if you do so relatively informally in some cases.

If you do not catch the project early enough to do a DPIA, this does not remove the need to comply properly with the GDPR and Data Protection Act 2018, the Human Rights Act 1998 (as it applies to privacy), duties of confidentiality and proper standards of information security. Dodging or avoiding a DPIA is highly likely to result in greater expense later on, either by solutions or extra stages bolted onto the project later, or by fines, enforcement or other action taken because the project and how it works are non-compliant.

3 Do we need to do a DPIA?

3.1 Is our project the right kind of project?

DPIAs apply to new or changing developments that affect the gathering or processing of personal data. Examples are likely to include:

- Procurement of a new database, or other new electronic system
- The introduction of monitoring (e.g. CCTV, email or internet monitoring, tracking of vehicles, equipment or especially people)
- Gathering special categories or other sensitive data, or changing the way it is gathered
- Changes to the design of an existing system in such a way that the nature of the data stored and the way it is accessed or used can be altered
- Existing systems and databases being merged
- Introduction of a new policy, procedure or service that changes the way in which personal information is used
- Changes to a policy or procedure that affects service users, staff or other individuals
- Allowing a new service, department or organisation to access an existing system
- Contracting out or outsourcing a service involving the use of personal data

If any of these apply to what you are doing, you may need to do a DPIA.

3.2 Is our project going to affect the way in which personal information is going to be used?

There are four situations where an impact assessment is mandatory:

- Using systematic profiling or automated decision-making to make significant decisions about people

- Processing special category data or criminal data on a large scale

- Systematically monitoring a publicly accessible place on a large scale

- Processing is otherwise considered to be 'high risk'

Applying these high-level descriptions to real proposals requires several

things to be unpacked.

'Systematic': for both the first and third criteria, "Systematic" means that the profiling / monitoring is ongoing and regular, rather than ad hoc or in response to specific events or circumstances.

'Large scale': for the second and third criteria, nobody has come up with a satisfactory definition of 'large scale', despite the fact that both the ICO and the European Data Protection Board have looked at it. Subsequent debates have confirmed that nobody has any intention of setting a number or proportion of data subjects that constitutes large scale. However you slice it, deciding whether processing is being done on a large scale is a subjective decision. The EDPB lists factors to take into account – the number of people, the volume of data being processed, the duration of the processing and the geographical area covered by it – but in the end, you just have to make a decision and document how you came by it. I think any processing involving more than 1000 people is large scale, but I'm aware that this is my instinct rather than anything else.

'Profiling' is the use of computer programs to analyse people or predict their behaviour – storing data electronically is not enough, the program that is being used has to create new data about the people being analysed. Automated decision-making requires a decision about the person to be made by the program – it is not a case of the data being presented to a human who makes the decision instead. The fear here is that if an analysis or decision is made by a person, the amount of data that can be taken into account is limited, and the subject of the decision has – at least in theory – the opportunity to talk to and influence that person. A machine can take enormous amounts of data, see patterns and coincidences that a human brain wouldn't have the capacity, and the opportunity to influence the program is limited.

A 'publicly accessible place' is any place that the public have regular access to – it could be private property like a shopping centre as well as a street or a public building.

3.3 High Risk?

The trickiest of the four to understand is what constitutes 'high risk' processing. At the time of writing, the Information Commissioner has published a list of situations which require a DPIA to be carried out, and the European Data Protection Board have done the same. Their conclusions are

not the same. The ICO – perhaps predictably – have adopted a more simplistic list of situations where an impact assessment is mandatory, whereas the EDPB approach is more fluid and unpredictable, listing criteria that *might* trigger an impact assessment but only where at least two apply.

The difference between the two lists might not be massively important to your organisation, especially if you decide that a broad approach is acceptable. By adopting the ICO model, you might end up doing more DPIAs than strictly necessary, but the consequence of this is – in my opinion – a win. DPIAs are a good way to head off negative consequences and wasted resources even if the risk of the project is lower than the threshold required to make one mandatory. However, if your priority is to make sure that you do what's required, the EDPB list is arguably the standard as the UK is still part of the EU at the time of writing, and the EDPB has asked to the UK to change their list.

In any case, it's worth looking at both lists to get a sense of the situations where you need to make sure that a DPIA is carried out. Key themes definitely emerge – using sensitive data in new situations, combining data in unexpected ways, processing data about vulnerable people – because they are common to both.

3.4 The ICO list (repeated without change):

- Innovative technology: processing involving the use of innovative technologies, or the novel application of existing technologies (including AI). A DPIA is required where this processing is combined with any of the criteria from the European guidelines.
- Denial of service: decisions about an individual's access to a product, service, opportunity or benefit that is based to any extent on automated decision-making (including profiling) or involves the processing of special category data.
- Large-scale profiling: any profiling of individuals on a large scale.
- Biometrics: any processing of biometric data. A DPIA is required where this processing is combined with any of the criteria from the European guidelines.
- Genetic data: any processing of genetic data, other than that processed by an individual GP or health professional for the provision of health care direct to the data subject. A DPIA is required where this processing is combined with any of the criteria from the European guidelines.
- Data matching: combining, comparing or matching personal data

obtained from multiple sources.

- Invisible processing: processing of personal data that has not been obtained direct from the data subject in circumstances where the controller considers that compliance with Article 14 would prove impossible or involve disproportionate effort. A DPIA is required where this processing is combined with any of the criteria from the European guidelines.
- Tracking: processing which involves tracking an individual's geolocation or behaviour, including but not limited to the online environment. A DPIA is required where this processing is combined with any of the criteria from the European guidelines.
- Targeting of children or other vulnerable individuals: the use of the personal data of children or other vulnerable individuals for marketing purposes, profiling or other automated decision-making, or if you intend to offer online services directly to children.
- Risk of physical harm: where the processing is of such a nature that a personal data breach could jeopardise the [physical] health or safety of individuals.

3.5 The EDPB factors (AKA the European guidelines in the ICO list above)

The EDPB approach is to examine a list of factors, and where two are combined, a DPIA is necessary:

- Evaluation or scoring
- Automated decisions with a legal or similarly significant effect
- Systematic monitoring of data subjects
- Processing of sensitive data (which includes special categories data, but also includes criminal data, and location or financial data)
- Large scale processing (which is not defined further than as mentioned above)
- Matching datasets from different processing activities
- Processing data about vulnerable subjects – this would include people have physical or mental health conditions or disabilities, but also extends to children and subjects who suffer from a power imbalance with the data controller. This means that employees, tenants and other people whose ability to consent meaningfully would be impaired by the power relationship
- The use of innovative processing techniques – this could the use of biometrics or so-called 'internet of things' devices like smart meters
- Processing that limits rights – any processing that involves assessing a person's eligibility for a contract or service would fall into this category

Unlike the ICO's list, the EDPB approach leaves the data controller with more discretion and forces the organisation to exercise more judgement.

3.6 What should we do now?

Regardless of whether you're trying to cover the mandatory elements alone, or capture a wider pool of projects, you need to develop criteria that make sense to your colleagues and disseminate them as far as you can. The bigger the organisation, the more difficult it might be to keep track of what people are planning to do. Therefore, you need to spread the message to decision and policymakers, project managers and those working in procurement. Below is a list of questions to get you started.

Are we obtaining new information from people or using data for new purposes?	
Are we using or sharing data about people without their knowledge? knowledge?	
Are we obtaining new information about people from other organisations?	
Are we sharing personal data with new organisations?	
Are we taking personal data that we already hold, and using it for something new?	
Are we using new technology that allows us to use information about people in a different way?	
Are we introducing any kind of routine surveillance, or widening the scale or scope of routine surveillance?	
Are we introducing any kind of monitoring e.g. of correspondence, behaviour or lifestyle, or widening its scope?	
Will we be using personal data as part of a process that involves significant decisions that will have an impact on the people whose data we are using? Might they be denied a service, or contract?	
Are we using information about people that they would consider to be secret or private?	
Are we using information about people that would cause them distress or damage if it was lost or stolen?	
Are we using information about people in a way that would put them at risk if the information was lost or stolen?	
Are we going to contact people in a new, unexpected way?	
Are we using data about people who are vulnerable e.g. children, people with physical or mental health conditions, refugees or	

asylum seekers, or other people who are at risk?	
Are we using data about people over whom we have power, or about whom we can make decisions without their consent e.g. employees, tenants or other individual people with whom we have a contractual relationship?	

If the answer to any of these questions is yes, a DPIA is very likely to be helpful, and may be mandatory.

4 The process

How you organise your DPIA should suit your internal procedures - as long as you can demonstrate that your DPIA follows the four-part structure set out by the GDPR, you've ticked that box and can concentrate on getting a positive practical outcome. There is an expectation that you will produce interim reports and a final summary report setting out risks that have been identified, and how they have been addressed, but that depends on how long the project runs and how often it changes. The DPIA is a living process – if the design of the project changes halfway through, a DPIA carried out at the beginning is no longer valid. Be prepared for several iterations of the DPIA, depending on how fluid and evolving the project turns out to be – a project may take a sudden turn and involve an increase of risk at a late stage, so the people responsible for the project need to be prepared for this.

The outputs are less important than the effect of identifying and dealing with risks. The objective for a DPIA is to ensure the risk assessment is built into the design and development of your project, with properly documented evidence of what risks you identified, and what treatments you chose to deal with them.

Look at the internal processes or procedures that would normally be followed to plan, approve and implement your project (NB, there is a risk that your organisation will not be compliant with Data Protection if the project development / management process cannot be laid out for you). Ensure that the DPIA forms a part of how the project is developed.

4.1 Who should carry out the DPIA?

The people best placed to carry out the DPIA will be those who own, design, develop and implement the project. They will understand why the project exists, what its objectives are, and what the intended effect will be. The

person carrying out the DPIA must be able to balance their understanding of the project against the following:

- Awareness of the legal framework (DPA, privacy, confidentiality)
- Awareness of the risks associated with the handling of data
- Willingness to identify and accept that the specific project involve risk

The GDPR is plainly not drafted with the expectation that the DPO will carry out the DPIA, and it is unlikely that any DPO would be sufficiently well-informed to carry out the first stage of writing a systematic description of the DPIA. It is nevertheless possible that the other stages could be carried out with the close involvement of the DPO, and even have the DPO deliver them. This is plainly an inversion of what the GDPR and EDPB guidance anticipated, but it should not represent a conflict of interest, which would be the biggest barrier to the DPO's involvement. The DPO will not determine the purposes of data processing; the people responsible for the project should have already done that, and if they haven't, nothing should happen until they do. They may give advice on the means of the processing if they are suggesting or advising on safeguards, but as a long as they do not make any decisions. The ideal DPIA is run by the project team, taking responsibility for risks that their project represents, supported by advice from the DPO. It may take a while to get there, and some people may always need to be persuaded / cajoled into carrying the DPA out.

The people running the DPIA must strike a balance between delivering the project on time and on budget and ensuring that it does not interfere with privacy in a disproportionate way or infringe the law.

4.2 Consultation

Virtually every model of DPIA / PIA in the world – including the DPIA model previously adopted in the UK as good practice – includes the use of consultation with affected stakeholders. Sometimes, this consultation will be internal. Those designing the project will understand what it is intended to do but may unable (or unwilling) to see unintended consequences or external risks. The project team must consult other teams and experts within the organisation to get their perspective, especially on the possible risks but also on the possible (and most appropriate) solutions.

More uncomfortably, the DPIA model usually asks those running it to consult externally. The GDPR does not make this mandatory in every case, but A35(9) does say that '*where appropriate*' the controller should seek the view of

affected data subjects or their representatives. This can be carried out with due regard to commercial confidentiality and other legitimate public interest reasons to keep some aspects of the project secret.

This means finding a representative sample of data subjects. It may also include trade unions, professional bodies, the police, the Information Commissioner or other regulators. Those who get consulted are not offered a veto on the project – the decisions about what to do are the responsibility of the project team, and the controller that they work for. However, affected data subjects are likely to have a perspective that is not available internally – they are not wedded to the project itself, or necessarily loyal to the data controller. They may use the opportunity to complain, or react sceptically to change, but they are equally like to identify risks that will impair or derail the project if not properly dealt with. Their views should be obtained as a matter of routine, and it may be worth consulting them more than once to ensure that changes to the project are also externally scrutinised.

4 Describe the uses of information

To carry out your DPIA, you need a clear, detailed explanation of what the project is intended to do, and how it works. As before, if this does not already exist, there is a strong chance that the organisation will not be compliant with the law more generally. The following questions are generic – you will need a detailed picture of how data is being used, tailored to the

- What is the project intended to achieve?
- What will the project allow you to do that you cannot do now?
- What will you learn about people that you do not already know, either by obtaining new information or combining existing information in a new format?
- Is delivering the project objectives mandatory or optional?
- What information is gathered?
- How is it gathered and where / who from?
- How are people informed about how their data is used?
- How is it stored?
- What security is in place?
- Who will have access to it, and how will they get access to it?
- How is the data transferred and shared?
- Who with?
- How long is the data retained?
- How is the data disposed of?

5 Assess the necessity and proportionality of the processing

For the processing to be necessary, the data controller needs to be able to show that there is not a reasonable alternative to the processing, that the project outcomes cannot be achieved by other means that involve less, or even no personal data being processed at all.

The CNIL guide to DPIAs emphasises the importance of assessing the GDPR implications at this stage:

- what is the purpose for processing the data?
- what is your legal basis for processing the data (and if special categories data, what is your exemption for processing the data?)
- how have you informed the data subjects (or what is your justification for not doing so?)
- what steps have you taken to comply with the other principles?

Once you understand how data is intended to be used, you have to consider two issues – what are the risks associated with how the data is intended to be used, and what might go wrong?

6 Risks

Some of the risks set out below are specific risks that would have to be prevented i.e. 'Individuals are not being adequately informed about the use of their data'. Some, like 'Data will be used on mobile devices will need to be mitigated or perhaps simply acknowledged / accepted. It is also important to take into account that mitigation may involve the proper application of existing procedures. Finally, the list below is generic and short, but might help to get the project team started.

SET-UP AND OBTAINING DATA

- Individuals are not being adequately informed about the use of their data
- You have decided not to tell people that their data is being used, but you do not have an exemption from the DP duty to inform people
- You have not identified a data protection condition (NB, if processing sensitive data, you will need a sensitive data condition)
- Consent is clearly required, but you are using an opt-out model
- People may be less willing to provide you with information if they find out how it will be used
- People may be less willing to engage with your organisation generally

if they find out how their data will be used

DATA USE

- The project will allow you to draw inferences, make assumptions or confirm things about the subject that they have not told you and do not know that you can work out – this might be your objective, which creates one set of issues, or it may be a by-product of the project and something you want to prevent
- The use of data is in some way governed by another organisation's policies or instructions (e.g. a requirement to provide data to government) leading to a loss of an autonomy for the subjects
- Data storage carries a risk of loss or theft
    - Data will be stored / maintained / used by Data Processors
    - Data will be stored / maintained / used by another Data Controller
    - Data will be stored remotely / in the cloud
    - Data will be routinely used in staff's homes
    - Data will be routinely used on staff's own devices
    - Data will be routinely used out of the office
    - Data will be routinely shared with external organisations
    - Data will be routinely shared with the public

DATA QUALITY

- Data is received in an incomplete manner
- Data is received in an unverified form
- Data is sourced only from a third party and we cannot verify it with the subject itself
- Data is historic and may be out of date
- Data is partial and may be inaccurate or inadequate
- There is no proper retention schedule for the data, so it may be kept for longer than is fair or not for long enough (for example, it is worth looking at the effect of the Home Office deleting data about those who came to the UK in the Windrush era)

RESILIENCE

- Data may not be backed up
- Data may not be encrypted or properly protected

SECURITY

- Access to the data is not properly controlled (e.g. there are no audit trails, users do not have to change passwords)
- The project design does not ensure that all staff who need access to the data have access
- We cannot control access to the premises where our data will be stored

7 Risk treatments

No guidance can tell you what to do if a risk or problem is identified. The DPIA model offers three different types of approach, and while they are very broad, you should ensure that understand why the approach has been taken. To decide what action to take, you need to balance the likely harm / damage / level of intrusion that the problem represents against the availability of solutions and their impact of your project. If something would be unfair and intrusive, and a small change to your project would remove that unfairness or intrusion, you must immediately make the change. Conversely, if there will be some mild effect but avoiding it will derail the project altogether, you may decide to acknowledge the risk but leave it untreated.

7.1 Prevent / avoid

If you identify a risk that is intolerable or unacceptable, or if any risk can be removed without significant effect on the project (even if the risk itself is relatively minor), you should alter the design of the project to remove the risk. The importance of considering this approach must not be underestimated. The purpose of carrying out a DPIA when the project is still being designed is precisely because it will still be possible to make the change.

7.2 Mitigate

It might be appropriate to put in place a measure to mitigate the risk, which means doing something to reduce the likelihood of the risk from occurring or reducing the effect. If staff are using laptops to access sensitive data, there is a risk that it might be lost, and any data stored on it might be accessed. Disabling the hard drive to prevent data storage in the first place probably prevents the risk. Encrypting the hard drive mitigates the risk – the data is still stored on the machine, but it much less likely to be accessed by anyone

finding it. However, this only mitigates one aspect of the risk. The data may not be backed up if stored on the laptop, and the data is still accessible if the password is not sufficiently strong.

7.3 Acknowledge / accept

The old ICO PIA Code of Practice explicitly allowed some risks to be acknowledged or accepted, which means recording and considering the risk but not taking any steps. The most obvious circumstances where accepting a risk will occur is where the risk itself is unlikely to be realised, its effects would be limited or (especially) a combination of the two. It is also possible that the risk is more serious, but there is no available solution that will allow the project to go ahead. This is a significant decision – you will have to acknowledge that the importance of the project or its overall benefits outweigh the risk to the privacy of individuals. Especially if you publish the DPIA report (which is the norm) or if you are covered by the Freedom of Information Act, it is quite likely that this decision will become public. You have to be willing to justify this kind of decision to the people who might be affected.

It is pointless to carry out a DPIA on something that is being imposed on you from outside, and which you cannot materially change, and this represents a problem if you believe that the criteria for a mandatory are met. For example, if the new project is being developed because of a legal obligation or a government / regulatory requirement and you have to implement it in the way that they tell you to, a DPIA will be a waste of time for practical purposes. You should concentrate on developing corporate or local policies and procedures to protect and properly use personal information if you cannot change the design of the project. Your DPIA may focus on aspects of a project that you have flexibility over, even if others are out of your control, and you might get the benefit there. However, if you identify high risks with no obvious solution in these circumstances, the door is opened to Prior Consultation.

8 Prior consultation

The circumstances where prior consultation will be necessary are limited. Article 36 states that prior consultation is required only where a high risk has been identified during a DPIA which cannot be mitigated (this is confirmed in Recital 94). If there is a significant risk but the project team and DPO are satisfied that it can be effectively managed, prior consultation is not required.

Alternatively, if no obvious solution exists and the team / data controller are determined to go ahead, prior consultation is mandatory and the ICO could issue a monetary penalty for the failure to consult. How prior consultation is a mystery – the ICO has not announced the outcome of any particular instance of it, and at the time of writing, no action has been announced as a consequence of it.

The process is straightforward – the organisation emails a list of information specified by the Commissioner on their website, and the ICO has eight weeks (which can be extended by up to six additional weeks in complex cases) to give their view. This could be anything from confirmation that the risks have been properly managed after all, through advice about possible changes, all the way to an order (via an enforcement notice) not to alter the project or even not process the data at all.

The crucial thing about prior consultation is that if surrendering the fate of your project to the ICO sounds undesirable, an intelligent and effective solution to the risk, a change to the way the project works, or even a pause before implementation will all avoid the need to carry it out.