Information Commissioner's Office

Consultation:
GDPR DPIA guidance

Start date: 22 March 2018
End date: 13 April 2018

ico.
Information Commissioner's Office

ICO GDPR guidance:
Data Protection Impact Assessments (DPIAs)

Contents (for web navigation bar)

At a glance

- A data protection impact assessment (DPIA) is a process to help you identify and minimise the data protection risks of a project.

- You must do a DPIA for certain types of processing, or any other processing that is **likely to result in a high risk** to individuals. You can use our screening checklists to help you decide when to do a DPIA.

- It is also good practice to do a DPIA for any other major project which requires the processing of personal data.

- Your DPIA must:

    - describe the nature, scope, context and purposes of the processing;
    - assess necessity, proportionality and compliance measures;
    - identify and assess risks to individuals; and
    - identify any additional measures to mitigate those risks.

- To assess the level of risk, you must consider both the likelihood and the severity of any impact on individuals. High risk could result from either a high probability of some harm, or a lower possibility of serious harm.

- You should consult your data protection officer (if you have one) and, where appropriate, individuals and relevant experts. Any processors may also need to assist you.

- If you identify a high risk that you cannot mitigate, you must consult the ICO before starting the processing.

- The ICO will give written advice within eight weeks, or 14 weeks in complex cases. If appropriate, we may issue a formal warning not to process the data, or ban the processing altogether.

Key provisions in the GDPR
See Articles 35 and 36 and Recitals 74-77, 84, 89-92, 94 and 95

Further reading – ICO guidance

We have published more detailed guidance on DPIAs. The content of this detailed guidance is subject to public consultation, which closes on 13 April 2018.

Further reading – Article 29 guidelines

The Article 29 Working Party includes representatives from the data protection authorities of each EU member state. It adopts guidelines for complying with the requirements of the GDPR.

The working party has published Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 (WP248).

Other relevant guidelines include:

Guidelines on Data Protection Officers ('DPOs') (WP243)

Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679 (WP251)

About this detailed guidance

These pages sit alongside our Guide to the GDPR and provide more detailed guidance for UK organisations on data protection impact assessments (DPIAs) under the GDPR. They replace our previous code of practice on conducting privacy impact assessments.

DPIAs are a tool to help you identify and minimise the data protection risks of new projects. They are part of your accountability obligations under the GDPR, and an integral part of the 'data protection by default and by design' approach. An effective DPIA helps you to identify and fix problems at an early stage, demonstrate compliance with your data protection obligations, meet individuals' expectations of privacy and help avoid reputational damage which might otherwise occur. In some cases the GDPR says you must carry out a DPIA, but they can be a useful tool in other cases too.

This guidance explains the principles and process that form the basis of a DPIA. It helps you to understand what a DPIA is for, when you need to carry one out, and how to go about it. It also explains the role of the ICO, when you have to consult us, and how that consultation process works.

The process described in this guidance is designed to be flexible enough to work for organisations of any size and in any sector – although if you are processing for law enforcement purposes you should read this alongside the Guide to law enforcement processing. If you are likely to conduct regular DPIAs, you can also use this guidance as a starting point to develop your own bespoke DPIA process and methodology which fits with your particular needs and existing working practices.

For an introduction to the key themes and provisions of the GDPR, including broader accountability obligations, you should refer back to the Guide to the GDPR. You can navigate back to the Overview at any time using the link on the left hand side of this page. Links to other relevant guidance and sources of further information are also provided throughout.

When downloading this guidance, the corresponding content from the Guide to the GDPR will also be included so you will have all the relevant information on this topic.

What's new under the GDPR?

In brief...

The GDPR introduces a new obligation to do a DPIA before carrying out types of processing likely to result in high risk to individuals' interests. If your DPIA identifies a high risk that you cannot mitigate, you must consult the ICO.

This is a key element of the new focus on accountability and data protection by design.

Some organisations already carry out privacy impact assessments (PIAs) as a matter of good practice. If so, the concept will be familiar, but you still need to review your processes to make sure they comply with GDPR requirements. DPIAs are now mandatory in some cases, and there are specific legal requirements for content and process.

If you have not already got a PIA process, you need to design a new DPIA process and embed this into your organisation's policies and procedures.

In the run-up to 25 May 2018, you also need to review your existing processing operations and decide whether you need to do a DPIA, or review your PIA, for anything which is likely to be high risk. You do not need to do a DPIA if you have already considered the relevant risks and safeguards in another way, unless there has been a significant change to the nature, scope, context or purposes of the processing since that previous assessment.

In more detail...

Is this a new obligation?

Yes, the GDPR includes a new obligation to conduct a DPIA for types of processing likely to result in a high risk to individuals' interests.

This is part of the new focus on accountability and being able to demonstrate that you comply with the GDPR. It is a key element of data protection by design and by default, and also reflects the more risk-based approach to data protection obligations taken throughout the GDPR.

Relevant provisions in the GDPR
See Articles 24, 25, 35 and 36 and Recitals 74-95

What should we do if we already carry out PIAs?

Privacy impact assessments (PIAs) have been used for a number of years as a good practice measure to identify and minimise privacy risks associated with new projects. DPIAs are very similar to PIAs, so if you already carry out PIAs in accordance with our pre-existing PIA code, the new process will be very familiar.

However, you may need to adapt your internal policies, processes and procedures to ensure they meet the requirements for DPIAs under the GDPR. The key changes include:

- DPIAs are mandatory for any processing likely to result in a high risk (including some specified types of processing). You need to review your screening questions to make sure you comply with the new requirements.

- You must consider the impact on any of an individuals' rights and freedoms, including (but not limited to) privacy rights.

- There are more specific requirements for the content of a DPIA.

- You must seek the advice of your data protection officer (DPO), if you have one. You also need to seek the views of people whose data you intend to process, or their representatives, wherever possible.

- If after doing a DPIA you conclude that there is a high risk and you cannot mitigate that risk, you must formally consult the ICO before you can start the processing.

What should we do if we don't already carry out PIA's?

If you don't have an existing PIA process, you need to ensure that you understand DPIA requirements and embed them into your business practices. If you are likely to carry out lots of DPIAs, you may want to consider using this guidance as a starting point to design a bespoke DPIA process to meet your specific needs and fit with your existing organisational practices.

You should also review your existing processing operations to identify whether you already do anything that would be considered likely high risk under the GDPR. If so, are you confident that you have already adequately assessed and mitigated the risks of that project? If not, you may need to conduct a DPIA now to ensure the processing complies with the GDPR. However, the ICO does not expect you to do a new DPIA for established processing where you have already considered relevant risks and safeguards (whether as part of a PIA or another formal or informal risk assessment process) - unless there has been a significant change to the nature, scope, context or purposes of the processing since that previous assessment.

We recommend that you document your review and your reasons for not conducting a new DPIA where relevant, to help you demonstrate compliance if challenged.

Relevant provisions in the GDPR
See Articles 35 and 36 and Recitals 84 and 89-95

Further reading
The Article 29 Working Party includes representatives from the data protection authorities of each EU member state. It adopts guidelines for complying with the requirements of the GDPR.

The working party has adopted Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 (WP248). In particular, Annex 2 sets out a detailed checklist for DPIA methodology.

What is a DPIA?

In brief...

A DPIA is a way for you to systematically and comprehensively analyse your processing and help you identify and minimise data protection risks.

DPIAs should consider compliance risks, but also broader risks to the rights and freedoms of individuals, including the potential for any significant social or economic disadvantage. The focus is on the potential for harm –- to individuals or to society at large, whether it is physical, material or non-material.

To assess the level of risk, a DPIA must consider both the likelihood and the severity of any impact on individuals.

A DPIA does not have to eradicate the risks altogether, but should help to minimise risks and assess whether or not remaining risks are justified.

DPIAs are a legal requirement for processing that is likely to be high risk. But an effective DPIA can also bring broader compliance, financial and reputational benefits, helping you demonstrate accountability and building trust and engagement with individuals.

A DPIA may cover a single processing operation or a group of similar processing operations. A group of controllers can do a joint DPIA.

It's important to embed DPIAs into your organisational processes and ensure the outcome can influence your plans. A DPIA is not a one-off exercise and you should see it as an ongoing process, and regularly review it.

In more detail...

What is a DPIA?

A DPIA is a process designed to help you systematically analyse, identify and minimise the data protection risks of a project or plan. It is a key part of your accountability obligations under the GDPR, and when done properly helps you assess and demonstrate how you comply with all of your data protection obligations.

It does not have to eradicate all risk, but should help you minimise and determine whether or not the level of risk is acceptable in the circumstances, taking into account the benefits of what you want to achieve.

DPIAs are designed to be a flexible and scalable tool that you can apply to a wide range of sectors and projects. Conducting a DPIA does not have to be complex or time-consuming in every case, but there must be a level of rigour in proportion to the privacy risks arising.

There is no definitive DPIA template that you must follow. You can use our suggested template if you wish, or you may want to develop your own template and process to suit your particular needs, using this guidance as a starting point.

Relevant provisions in the GDPR
See Articles 35(1) and 35(7) and Recitals 84 and 90

Why are DPIAs important?

DPIAs are an essential part of your accountability obligations. Conducting a DPIA is a legal requirement for any type of processing that is likely to result in high risk (including certain specified types of processing). Failing to carry out a DPIA in these cases may leave you open to enforcement action, including a fine of up to €10 million, or 2% global annual turnover if higher.

A DPIA also brings broader compliance benefits, as it can be an effective way to assess and demonstrate your compliance with all data protection principles and obligations.

However, DPIAs are not just a compliance exercise. An effective DPIA allows you to identify and fix problems at an early stage, bringing broader benefits for both individuals and your organisation.

It can reassure individuals that you are protecting their interests and have reduced any negative impact on them as much as you can. In some cases the consultation process for a DPIA gives them a chance to have some say in the way their information is used. Conducting and publishing a DPIA can also improve transparency and make it easier for individuals to understand how and why you are using their information

In turn, this can create potential benefits for your reputation and relationships with individuals. Conducting a DPIA can help you to build trust and engagement with the people using your services, and improve your understanding of their needs, concerns and expectations.

There can also be financial benefits. Identifying a problem early on generally means a simpler and less costly solution, as well as avoiding potential reputational damage later on. A DPIA can also reduce the ongoing costs of a project by minimising the amount of information you collect where possible, and devising more straightforward processes for staff.

In general, consistent use of DPIAs increases the awareness of privacy and data protection issues within your organisation and ensures that all relevant staff involved in designing projects think about privacy at the early stages and adopt a 'data protection by design' approach.

Relevant provisions in the GDPR
See Articles 5(2), 24, 25, 35 and 83

How are DPIAs used?

A DPIA can cover a single processing operation, or a group of similar processing operations. You may even be able to rely on an existing DPIA if it covered a similar processing operation with similar risks. A group of controllers can also do a joint DPIA for a group project or industry-wide initiative.

For new technologies, you may be able to use a DPIA done by the product developer to inform your own DPIA on your implementation plans.

You can use an effective DPIA throughout the development and implementation of a project or proposal, embedded into existing project management or other organisational processes.

For new projects, DPIAs are a vital part of data protection by design. They build in data protection compliance at an early stage, when there is most scope for influencing how the proposal is developed and implemented.

However, it's important to remember that DPIAs are also relevant if you are planning to make changes to an existing system. In this case you must ensure that you do the DPIA at a point when there is a realistic opportunity to influence those plans. Recital 84 of the GDPR is clear that:

Quote
"the outcome of the assessment should be taken into account when determining the appropriate measures to be taken in order to demonstrate that the processing of personal data complies with this Regulation."

In other words, a DPIA is not simply a rubber stamp or a technicality as part of a sign-off process. It's vital to integrate the outcomes of your DPIA back into your project plan.

You should not view a DPIA as a one-off exercise to file away. A DPIA is a 'living' process to help you manage and review the risks of the processing and the measures you've put in place on an ongoing basis. You need to keep it under review and reassess if anything changes.

In particular, if you make any significant changes to how or why you process personal data, or to the amount of data you collect, you need to show that your DPIA assesses any new risks. An external change to the wider context of the processing should also prompt you to review your DPIA. For example, if a new security flaw is identified, new technology is made available, or a new public concern is raised over the type of processing you do or the vulnerability of a particular group of data subjects –.

Relevant provisions in the GDPR
See Articles 35(1) and 35(11), and Recitals 84 and 92

Further reading
The Article 29 Working Party includes representatives from the data protection authorities of each EU member state. It adopts guidelines for complying with the requirements of the GDPR.

The working party has adopted Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 (WP248).

What kind of 'risk' do they assess?

There is no explicit definition of 'risk' in the GDPR, but the various provisions on DPIAs make clear that this is about the risks to individuals' interests. Article 35 says that a DPIA must consider "risks to the rights and freedoms of natural persons". This includes risks to privacy and data protection rights, but also effects on other fundamental rights and interests.

The key provision here is Recital 75, which links risk to the concept of potential harm or damage to individuals:

Quote
"The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data…".

The focus is therefore on any potential harm to individuals. However, the risk-based approach is not just about actual damage and should also look at the possibility for more intangible harm. It includes any "significant economic or social disadvantage".

The impact on society as a whole may also be a relevant risk factor. For example, it may be a significant risk if your intended processing leads to a loss of public trust.

A DPIA must assess the level of risk, and in particular whether it is 'high risk'. The GDPR is clear that assessing the level of risk involves looking at both the likelihood and the severity of the potential harm.

For more guidance on what this all means in practice, see the section on how to carry out a DPIA.

Relevant provisions in the GDPR
See Article 35(1) and Recitals 4, 75, 76, 84 and 90

Further reading
The Article 29 Working Party includes representatives from the data protection authorities of each EU member state. It adopts guidelines for complying with the requirements of the GDPR.

The working party has adopted Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 (WP248) which include some discussion of the nature of risk.

See also the working party's Statement on the role of a risk-based approach in data protection legal frameworks (WP218, 30 May 2014).

When do we need to do a DPIA?

In brief…

You must do a DPIA before you begin any type of processing which is "likely to result in a high risk". This means that although you have not yet assessed the actual level of risk you need to screen for factors that point to the potential for a widespread or serious impact on individuals.

In particular, the GDPR says you must do a DPIA if you plan to:

- use systematic and extensive profiling with significant effects;
- process special category or criminal offence data on a large scale; or
- systematically monitor publicly accessible places on a large scale.

The ICO also requires you to do a DPIA if you plan to:

- use new technologies;
- use profiling or special category data to decide on access to services;
- profile individuals on a large scale;
- process biometric data;
- process genetic data;
- match data or combine datasets from different sources;
- collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing');
- track individuals' location or behaviour;
- profile children or target marketing or online services at them; or
- process data that might endanger the individual's physical health or safety in the event of a security breach.

You should also think carefully about doing a DPIA for any other processing that is large scale, involves profiling or monitoring, decides on access to services or opportunities, or involves sensitive data or vulnerable individuals.

Even if there is no specific indication of likely high risk, it is good practice to do a DPIA for any major new project involving the use of personal data.

Consultation – have your say
The ICO is required by Article 35(4) of the GDPR to publish a list of types of processing we consider likely to be high risk and so require a DPIA. Our list, which is summarised above, is currently open for consultation until 13 April 2018.

In more detail...

What is the general rule?

Article 35(1) says that you must do a DPIA where a type of processing is **likely to result in a high risk** to the rights and freedoms of individuals:

Quote
"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."

What does 'high risk' mean?

Risk in this context is about the potential for any significant physical, material or non-material harm to individuals. See What is a DPIA? for more information on the nature of the risk.

To assess whether something is 'high risk', the GDPR is clear that you need to consider both the likelihood and severity of any potential harm to individuals. 'Risk' implies a more than remote chance of some harm. 'High risk' implies a higher threshold, either because the harm is more likely, or because the potential harm is more severe, or a combination of the two. Assessing the likelihood of risk in that sense is part of the job of a DPIA.

However, the question for these initial screening purposes is whether the processing is **of a type likely to result in** a high risk.

What does 'likely to result in a high risk' mean?

The GDPR doesn't define 'likely to result in high risk'. However, the important point here is not whether the processing is actually high risk or likely to result in harm – that is the job of the DPIA itself to assess in detail. Instead, the question is a more high-level screening test: are there features which point to the potential for high risk? You are screening for any red flags which indicate that you need to do a DPIA to look at the risk (including the likelihood and severity of potential harm) in more detail.

Article 35(3) lists three examples of types of processing that automatically requires a DPIA, and the ICO has published a list under Article 35(4) setting out ten more. There are also European guidelines with some criteria to help you identify other likely high risk processing.

This does not mean that these types of processing are always high risk, or are always likely to cause harm – just that there is a reasonable chance they may be high risk and so a DPIA is required to assess the level of risk in more detail.

If your intended processing is not described under GDPR, Article 35(3) the ICO list or European guidelines then ultimately, it's up to you to decide whether your processing is of a type likely to result in high risk, taking into account the nature, scope, context and purposes of the processing. If in any doubt, we would always recommend that you do a DPIA to ensure compliance and encourage best practice.

What types of processing automatically require a DPIA?

Article 35(3) sets out three types of processing which always require a DPIA:

1. **Systematic and extensive profiling with significant effects:**

> **Quote**
> "(a) any systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person".

2. **Large scale use of sensitive data:**

> **Quote**
> "(b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10".

3. **Public monitoring:**

> **Quote**
> "(c) a systematic monitoring of a publicly accessible area on a large scale".

The ICO is required by Article 35(4) to publish a list of the kind of processing operations that are likely to be high risk and require a DPIA. Our list (currently open for consultation) includes a further ten types of processing that automatically require a DPIA:

1. **New technologies:** processing involving the use of new technologies, or the novel application of existing technologies (including AI).

2. **Denial of service:** Decisions about an individual's access to a product, service, opportunity or benefit which is based to any extent on automated decision-making (including profiling) or involves the processing of special category data.

3. **Large-scale profiling:** any profiling of individuals on a large scale.

4. **Biometrics:** any processing of biometric data.

5. **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].

6. **Data matching:** combining, comparing or matching personal data obtained from multiple sources.

7. **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.

8. **Tracking:** processing which involves tracking an individual's geolocation or behaviour, including but not limited to the online environment.

9. **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.

10. **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.

You should also be aware that the data protection authorities in other EU member states will publish lists of the types of processing that require a DPIA in their jurisdiction.

Relevant provisions in the GDPR
See Articles 35(3) and 35(4)

Consultation – have your say
The ICO is required by Article 35(4) of the GDPR to publish a list of types of processing we consider likely to be high risk and so require a DPIA. Our list is currently open for consultation until 13 April 2018.

What other factors might indicate likely high risk?

The Article 29 working party of EU data protection authorities has published guidelines with nine criteria which may act as indicators of likely high risk processing:

- Evaluation or scoring.
- Automated decision-making with legal or similar significant effect.
- Systematic monitoring.
- Sensitive data or data of a highly personal nature.
- Data processed on a large scale.
- Matching or combining datasets.
- Data concerning vulnerable data subjects.
- Innovative use or applying new technological or organisational solutions.
- Preventing data subjects from exercising a right or using a service or contract.

In most cases, a combination of two of these factors indicates the need for a DPIA. However, this is not a strict rule. You may be able to justify a decision not to carry out a DPIA if you are confident that the processing is nevertheless unlikely to result in a high risk, but you should document your reasons.

On the other hand, in some cases you may need to do a DPIA if only one factor is present – and it is good practice to do so.

For more guidance on these factors, read the Article 29 guidelines.

Further reading
WP29 Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 (WP248)

Relevant provisions in the GDPR
See Recitals 89 and 91

What does 'new technologies' mean?

The GDPR does not define 'new technologies'.

Recital 91 indicates that this concerns new developments to the state of technological knowledge in the world at large, rather than technology that is new to you. Using technology to process personal data in novel or unexpected ways is likely to be inherently more risky than using technologies that are tried and tested, as the practical implications will not yet be fully understood. This could include the application of artificial intelligence or machine learning within processing operations.

The Article 29 working party guidelines also suggest that the concept of new technologies includes the innovative application of existing technologies to process data in new ways or for new purposes.

If you are planning to use technology you have not used before, even if it is not brand new, we recommend that you still do a DPIA. The technology itself may have been tested by others, but you need to ensure that you understand the risks and implement it in the most privacy-friendly way – and it may still be considered a 'new technology' if you are actually using the existing technology in a new or innovative way. You may be able to rely to some extent on any earlier DPIAs carried out on existing technologies by the developer or by another controller who has already put it to use, but it is important to add on an assessment of your own specific implementation plans including the specific nature, scope, purposes and context of your processing. What is regarded as a new technology may vary by sector to sector, depending on the maturity of its use in that area.

Further reading
Read our paper on paper on big data, artificial intelligence, machine learning and data protection which contains further guidance on application of these technologies in a data protection context.

Relevant provisions in the GDPR
See Article 35(1) and Recitals 89 and 91

What does 'systematic and extensive' mean?

Again, the GDPR does not define 'systematic' or 'systematic and extensive'.

There is some guidance on the meaning of 'systematic' in European guidelines on the DPO provisions. The DPO guidelines say that 'systematic' means that the processing:

- occurs according to a system;
- is pre-arranged, organised or methodical;
- takes place as part of a general plan for data collection; or
- is carried out as part of a strategy.

The term 'extensive' implies that the processing also covers a large area, involves a wide range of data or affects a large number of individuals.

Further reading
The Article 29 working party of European data protection authorities has adopted Guidelines on Data Protection Officers ('DPOs') (WP243) which contain guidance on the meaning of the term 'systematic'.

Relevant provisions in the GDPR
See Article 35(3)(a) and (c) and Recital 91

What does 'significantly affect' mean?

The GDPR does not define the concept of a legal or similarly significant effect. However, Article 29 working party guidelines on this phrase in the context of profiling provisions give some further guidance.

In short, it is something that has a noticeable impact on an individual and can affect their circumstances, behaviour or choices in a significant way.

A legal effect is something that affects a person's legal status or legal rights. A similarly significant effect might include something that affects a person's financial status, health, reputation, access to services or other economic or social opportunities.

Decisions that have little impact generally could still have a significant effect on more vulnerable people, such as children.

Further reading
Read our guidance on profiling and automated decision-making for more on legal and similarly significant effects.
Read our guidance on children and the GDPR for more on significant effects specifically in relation to children and their personal data.

Further reading – Article 29

The Article 29 working party of European data protection authorities has adopted Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679 (WP251) which contain guidance on legal and similarly significant effects.

Relevant provisions in the GDPR
See Article 35(3)(a) and Recital 91

What does 'large scale' mean?

Again, the GDPR does not contain a definition of large-scale processing, but to decide whether processing is on a large scale you should consider:

- the number of individuals concerned;
- the volume of data;
- the variety of data;
- the duration of the processing; and
- the geographical extent of the processing.

Examples of large-scale processing include:

- a hospital (but not an individual doctor) processing patient data;
- tracking individuals using a city's public transport system;
- a fast food chain tracking real-time location of its customers;
- an insurance company or bank processing customer data;
- a search engine processing data for behavioural advertising; or
- a telephone or internet service provider processing user data.

Individual professionals processing patient or client data are not processing on a large scale.

Relevant provisions in the GDPR
See Articles 35(3)(b) and (c) and Recital 91

Further reading
The Article 29 working party has adopted two sets of guidelines including discussion of 'large scale':

Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 (WP248)

Guidelines on Data Protection Officers ('DPOs') (WP243)

Are there any exceptions?

You may not have to carry out a DPIA if:

- **You are processing on the basis of legal obligation or public task.** However, this exception only applies if:
    - you have a clear statutory basis for the processing;
    - the legal provision or a statutory code specifically provides for and regulates the processing operation in question;
    - you are not subject to other obligations to complete DPIAs, such as those required by Cabinet Office for consideration of information governance risks or requirements derived from specific legislation, such as Digital Economy Act 2017;
    - a data protection risk assessment was carried out as part of the impact assessment when the legislation was adopted. This may not always be clear, and in the absence of any clear and authoritative statement on whether such an assessment was conducted we recommend that you err on the side of caution and conduct a DPIA to ensure you consider how best to mitigate any high risk.
- **You have already done a substantially similar DPIA**. You need to be confident that you can demonstrate that the nature, scope, context and purposes of the processing are all similar.
- **The ICO issues a list of processing operations which do not require a DPIA.** We have the power to establish this type of list, but we have not done so yet. We may consider a list in future in the light of our experience of how the DPIA provisions are being interpreted in practice.

Relevant provisions in the GDPR
See Articles 35(4) and (10)

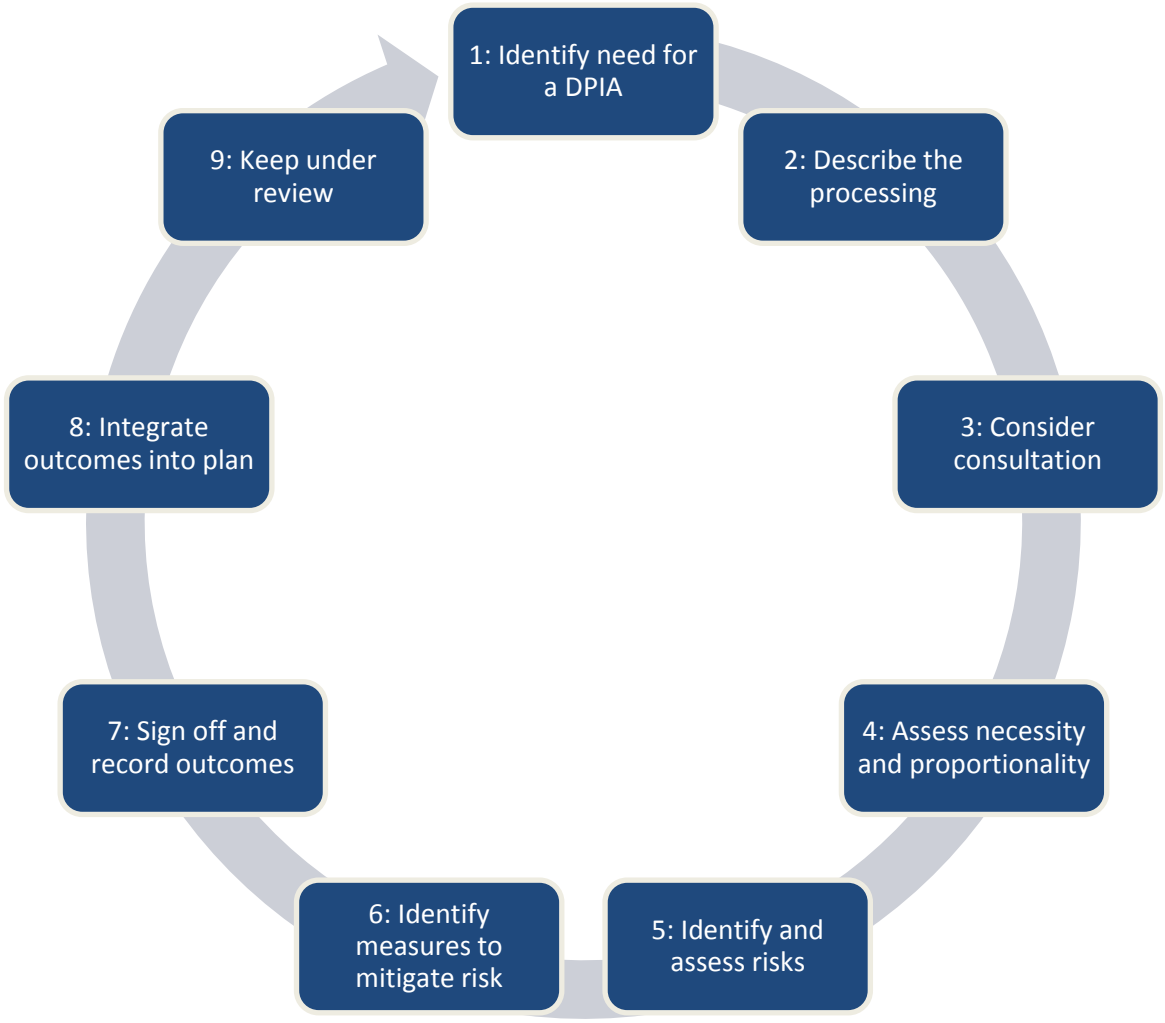
Further reading
WP29 Guidelines on Data Protection Impact Assessment (DPIA) and

determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679 (WP248)

How do we carry out a DPIA?

In brief...

A DPIA should begin early in the life of a project, before you start your processing, and run alongside the planning and development process. It should include these steps:



You must seek the advice of your data protection officer (if you have one). You should also consult with individuals and other stakeholders throughout this process.

The process is designed to be flexible and scalable. You can use or adapt our sample DPIA template, or create your own. If you want to create your own, you may want to refer to the European guidelines which set out Criteria for an acceptable DPIA.

We recommend that you publish your DPIAs, with sensitive details removed if necessary.

In more detail...

What are the key elements of a DPIA process?

A DPIA should begin early in the life of a project, before you start your processing, and run alongside the planning and development process. It should include these steps:

- Step 1: identify the need for a DPIA
- Step 2: describe the processing
- Step 3: consider consultation
- Step 4: assess necessity and proportionality
- Step 5: identify and assess risks
- Step 6: identify measures to mitigate the risks
- Step 7: sign off and record outcomes
- Step 8: integrate outcomes into project plan
- Step 9: keep your DPIA under review

You should consult with individuals and other stakeholders as needed throughout this process.

The DPIA process is designed to be flexible and scalable. You can design a process that fits with your existing approach to managing risks and projects, as long as it contains these key elements.

You can also scale the time and resources needed for a DPIA to fit the nature of the project. It does not need to be a time-consuming process in every case.

Relevant provisions in the GDPR
See Articles 35(2), (7) and (9)

Further reading
Annex 2 of WP29 Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 (WP248) sets out a checklist of criteria for an acceptable DPIA.

Is there a template we can use?

You can use or adapt our sample DPIA template if you wish.

You don't have to use this template. You can develop your own template to suit your own needs, or use existing project management methodology, as long as it covers all of the key elements of the process. If you are developing your own template, you might find it helpful to refer to the Criteria for an acceptable DPIA in Annex 2 of the Article 29 working party guidelines.

Who is responsible for the DPIA?

You can decide who has responsibility for carrying out DPIAs within your organisation, and who signs them off. You can outsource your DPIA, but you remain responsible for it. You may want to ask a processor to carry out a DPIA on your behalf if they undertake the relevant processing operation.

Who should be involved in the DPIA?

- a DPO, if you have one;
- information security staff;
- any processors; and
- legal advisors or other experts, where relevant.

Further reading
WP29 Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 (WP248)

What is the role of the DPO?

If you have a DPO, you must seek their advice. The DPO should provide advice on:

- whether you need to do a DPIA;
- how you should do a DPIA;
- whether to outsource the DPIA or do it in-house;
- what measures and safeguards you can take to mitigate risks;
- whether you've done the DPIA correctly; and
- the outcome of the DPIA and whether the processing can go ahead.

You should record your DPO's advice on the DPIA. If you don't follow their advice, you should record your reasons and ensure you can justify your decision.

DPOs must also monitor the ongoing performance of the DPIA, including how well you have implemented your planned actions to address the risks.

You may find that your DPO is best placed to take overall responsibility for the DPIA.

Relevant provisions in the GDPR
See Articles 35(2) and 39(1)(c)

Further reading
WP29 Guidelines on Data Protection Officers ('DPOs')

Step 1: How do we decide whether to do a DPIA?

Ask your DPO for advice. If you have any major project which involves the use of personal data it is good practice to carry out a DPIA. If you already intend to do a DPIA, go straight to step 2.

Otherwise, you need to check whether your processing is on the list of types of processing which automatically require a DPIA. If not, you need to screen for other factors which might indicate that it is a type of processing which is likely to result in high risk.

You can use or adapt the checklists at the end of this guidance to help you carry out this screening exercise. You can also read 'When do we need to do a DPIA?' for more guidance.

If you carry out this screening exercise and decide that you do not need to do a DPIA, you should document your decision and the reasons for it, including your DPO's advice. This does not have to be an onerous paperwork exercise ––as long as it helps you demonstrate that you have properly considered and complied with your DPIA obligations. For example, you could simply keep an annotated copy of the checklist

If you are in any doubt, we strongly recommend you do a DPIA.

Step 2: How do we describe the processing?

Describe how and why you plan to use the personal data. Your description must include "the nature, scope, context and purposes of the processing".

The nature of the processing is what you plan to do with the personal data. This should include, for example:

- how you collect the data;
- how you store the data;
- how you use the data;
- who has access to the data;
- who you share the data with;
- whether you use any processors;
- retention periods;
- security measures;
- whether you are using any new technologies;
- whether you are using any novel types of processing; and
- which screening criteria you flagged as likely high risk.

The scope of the processing is what the processing covers. This should include, for example:

- the nature of the personal data;

- the volume and variety of the personal data;
- the sensitivity of the personal data;
- the extent and frequency of the processing;
- the duration of the processing;
- the number of data subjects involved; and
- the geographical area covered.

The context of the processing is the wider picture, including internal and external factors which might affect expectations or impact. This might include, for example:

- the source of the data;
- the nature of your relationship with the individuals;
- the extent to which individuals have control over their data;
- the extent to which individuals are likely to expect the processing;
- whether they include children or other vulnerable people;
- any previous experience of this type of processing;
- any relevant advances in technology or security;
- any current issues of public concern; and
- in due course, whether you comply with any GDPR codes of conduct (once any have been approved under Article 40) or GDPR certification schemes.
- Whether you have considered and complied with relevant codes of practice.

The purpose of the processing is the reason why you want to process the personal data. This should include:

- your legitimate interests, where relevant;
- the intended outcome for individuals; and
- the expected benefits for you or for society as a whole.

Relevant provisions in the GDPR
See Article 35(7)(a) and Recitals 84 and 90 and 94

Step 3: Do we need to consult individuals?

You should seek the views of individuals (or their representatives) unless there is a good reason not to.

In most cases it should be possible to consult individuals in some form. However, if you decide that it is not appropriate to consult individuals then

you should record this decision as part of your DPIA, with a clear explanation. For example, you might be able to demonstrate that consultation would compromise commercial confidentiality, undermine security, or be disproportionate or impracticable.

If the DPIA covers the processing of personal data of existing contacts (for example, existing customers or employees), you should design a consultation process to seek the views of those particular individuals, or their representatives.

If the DPIA covers a plan to collect the personal data of individuals you have not yet identified, you may need to carry out a more general public consultation process, or targeted research. This could take the form of carrying out market research with a certain demographic or contacting relevant campaign or consumer groups for their views.

If your DPIA decision is at odds with the views of individuals, you need to document your reasons for disregarding their views.

Relevant provisions in the GDPR
See Article 35(9)

Further reading
See WP29 Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 (WP248)

Step 3: Do we need to consult anyone else?

If you use a data processor, you may need to ask them for information and assistance. Your contracts with processors should require them to assist.

You should consult all relevant internal stakeholders, in particular anyone with responsibility for information security.

We also recommend you consider seeking legal advice or advice from other independent experts such as IT experts, sociologists or ethicists where appropriate. However, there are no specific requirements to do so.

In some circumstances you might also need to consult the ICO once you have completed your DPIA. See the next section of this guidance for more information.

Relevant provisions in the GDPR
See Article 28(3)(f)

Further reading
See page 15 of WP29 Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 (WP248)

Step 4: How do we assess necessity and proportionality?

You should consider:

- Do your plans help to achieve your purpose?
- Is there any other reasonable way to achieve the same result?

The Article 29 guidelines also say you should include how you ensure data protection compliance, which are a good measure of necessity and proportionality. In particular, you should include relevant details of:

- your lawful basis for the processing;
- how you will prevent function creep;
- how you intend to ensure data quality;
- how you intend to ensure data minimisation;
- how you intend to provide privacy information to individuals;
- how you implement and support individuals rights;
- measures to ensure your processors comply; and
- safeguards for international transfers.

Further reading
See annex 2 of WP29 Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 (WP248)

Step 5: How do we identify and assess risks?

Consider the potential impact on individuals and any harm or damage that might be caused by your processing – whether physical, emotional or material. In particular look at whether the processing could possibly contribute to:

- inability to exercise rights (including but not limited to privacy rights);
- inability to access services or opportunities;
- loss of control over the use of personal data;
- discrimination;
- identity theft or fraud;
- financial loss;
- reputational damage;
- physical harm;
- loss of confidentiality;
- reidentification of pseudonymised data; or
- any other significant economic or social disadvantage

You should include an assessment of the security risks, including sources of risk and the potential impact of each type of breach (including illegitimate access to, modification of or loss of personal data).

To assess whether the risk is a high risk, you need consider both the likelihood and severity of the possible harm. Harm does not have to be inevitable to qualify as a risk or a high risk. It must be more than remote, but any significant possibility of very serious harm may still be enough to qualify as a high risk. Equally, a high probability of widespread but more minor harm might still count as high risk.

You must make an 'objective assessment' of the risks. You might find it helpful to use a structured matrix to think about likelihood and severity of risks:

Severity of impact				
	Serious harm	**Low risk**	**High risk**	**High risk**
	Some impact	**Low risk**	**Medium risk**	**High risk**
	Minimal impact	**Low risk**	**Low risk**	**Low risk**
		Remote	Reasonable possibility	More likely than not
		Likelihood of harm		

You might also want to consider your own corporate risks, such as the impact of regulatory action, reputational damage or loss of public trust.

Relevant provisions in the GDPR
See Article 35(7)(c) and Recitals 76 and 90

Step 6: How do we identify mitigating measures?

Against each risk identified, record the source of that risk. You should then consider options for reducing that risk. For example:

- deciding not to collect certain types of data;
- reducing the scope of the processing;
- reducing retention periods;
- taking additional technological security measures;
- training staff to ensure risks are anticipated and managed;
- anonymising or pseudonymising data where possible;

- writing internal guidance or processes to avoid risks;
- adding a human element to review automated decisions;
- using a different technology;
- putting clear data sharing agreements into place;
- making changes to privacy notices;
- offering individuals the chance to opt out where appropriate; or
- implementing new systems to help individuals to exercise their rights.

This is not an exhaustive list, and you may be able to devise other ways to help reduce or avoid the risks. You should ask your DPO for advice.

Record whether the measure would reduce or eliminate the risk. You can take into account the costs and benefits of each measure when deciding whether or not they are appropriate.

Step 7: How do we conclude our DPIA?

You should then record:

- what additional measures you plan to take;
- whether each risk has been eliminated, reduced, or accepted;
- the overall level of 'residual risk' after taking additional measures; and
- whether you need to consult the ICO.

You do not always have to eliminate every risk. You may decide that some risks, and even a high risk, are acceptable given the benefits of the processing and the difficulties of mitigation. However, if there is still a high risk, you need to consult the ICO before you can go ahead with the processing.

As part of the sign-off process, you should ask your DPO to advise on whether the processing is compliant and can go ahead. If you decide not to follow their advice, you need to record your reasons.

You should also record any reasons for going against the views of individuals or other consultees.

What happens next?

You must integrate the outcomes of your DPIA back into your project plans. You should identify any action points and who is responsible for implementing them. You can use the usual project management process to ensure these are followed through.

You should monitor the ongoing performance of the DPIA. You may need to cycle through the process again before your plans are finalised.

If you have decided to accept a high risk, either because it is not possible to mitigate or because the costs of mitigation are too high, you need to consult the ICO before you can go ahead with the processing. See the next section for more information on this consultation process.

It is good practice to publish your DPIA to aid transparency and accountability. This could help foster trust in your processing activities, and improve individuals' ability to exercise their rights. If you are concerned that publication might reveal commercially sensitive information, undermine security or cause other risks, you should consider whether you can redact (black out) or remove sensitive details, or publish a summary. Public authorities need to consider their freedom of information obligations, as privacy impact assessments are included in the definition documents for publication schemes for many public authorities.

You need to keep your DPIA under review, and you may need to repeat it if there is a substantial change to the nature, scope, context or purposes of your processing.

Relevant provisions in the GDPR
See Articles 35(11), 36(1) and 39(1)(c) and Recital 84

Further reading
WP29 Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 (WP248)

Do we need to consult the ICO?

In brief...

You don't need to send every DPIA to the ICO and we expect the percentage sent to us to be small. But you must consult the ICO if your DPIA identifies a high risk and you cannot take measures to reduce that risk. You cannot begin the processing until you have consulted us.

If you want your project to proceed effectively then investing time in producing a comprehensive DPIA may prevent any delays later, if you have to consult with the ICO.

You need to complete our online form and submit a copy of your DPIA. Once we have the information we need, we will generally respond within eight weeks (although we can extend this by a further six weeks in complex cases).

We will provide you with a written response advising you whether the risks are acceptable, or whether you need to take further action. In some cases we may advise you not to carry out the processing because we consider it would be in breach of the GDPR. In appropriate cases we may issue a formal warning or take action to ban the processing altogether.

In detail...

When do we need to consult the ICO?

If you have carried out a DPIA that identifies a high risk, and you cannot take any measures to reduce this risk, you need to consult the ICO. You cannot go ahead with the processing until you have done so.

The focus is on the 'residual risk' after any mitigating measures have been taken. If your DPIA identified a high risk, but you have taken measures to reduce this risk so that it is no longer a high risk, you do not need to consult the ICO.

Relevant provisions in the GPDR
See Article 36(1) and Recital 94

Further reading
See page 18 of WP29 Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 (WP248)

How do we consult the ICO?

Complete our online form and submit a copy of your DPIA. You must include:

- a description of the respective roles and responsibilities of any joint controllers or processors;
- the purposes and methods of the intended processing;
- the measures and safeguards taken to protect individuals;
- contact details of your DPO;
- a copy of the DPIA; and
- any other information we ask for.

Relevant provisions in the GDPR
See Article 36(3)

What happens next?

When we receive your DPIA, we will check that we have all of the information we need.

We will also conduct a brief screening exercise to check that your DPIA does identify a high risk that has not been mitigated. If there is no residual high risk, we will let you know that we don't need to review the DPIA.

You should expect to be notified if your DPIA has been accepted for consultation within ten days of sending it to us.

If we agree that a DPIA was required, we will review your DPIA once we have all of the information we need. We will consider whether:

- the processing complies with data protection requirements;
- risks have been properly identified; and
- risks have been reduced to an acceptable level.

Relevant provisions in the GDPR
See Article 36(2)

How long does it take?

In most cases we will get back to you within eight weeks. In complex cases we may extend this to a maximum of 14 weeks. If we need to extend the deadline, we will tell you within one month of the date you submitted your DPIA and explain our reasons.

If we need to ask for additional information, the clock will stop until you provide the requested details.

In certain circumstances, were your intended processing operation would impact on data subjects in EU member states, we may be required to co-operate with other data protection authorities before provided our written advice, in accordance with chapter VII GDPR. Where this occurs it may mean that your case cannot be resolved in 14 weeks. We will notify you if this occurs and keep you updated.

Relevant provisions in the GDPR
See Article 36(2)

What are the possible outcomes?

We will provide you a written response, advising you that:

- the risks are acceptable and you can go ahead with the processing;
- you need to take further measures to reduce the risks;

- you have not identified all risks and you need to review your DPIA;
- your DPIA is not compliant and you need to repeat it; or
- the processing would not comply with the GDPR and you should not proceed.

In some cases, we may take more formal action. This might include an official warning not to proceed, or imposing a limitation or ban on processing.

In some cases, our draft decisions could be considered by other European data protection authorities where the scope of your intended processing includes European member states.

Relevant provisions in the GDPR
See Articles 36(2) and 58

Can we appeal?

If you disagree with our advice you can ask us to review our decision.

If you want to appeal against any formal action we may take, you should first ask us to review our decision. If you are still not happy, you can appeal to the First Tier Tribunal in certain cases .

DPIA checklists

DPIA awareness checklist

- ☐ We provide training so that our staff understand the need to consider a DPIA at the early stages of any plan involving personal data.
- ☐ Our existing policies, processes and procedures include references to DPIA requirements.
- ☐ We understand the types of processing that require a DPIA, and use the screening checklist to identify the need for a DPIA, where necessary.
- ☐ We have created and documented a DPIA process.
- ☐ We provide training for relevant staff on how to carry out a DPIA.

DPIA screening checklist

- ☐ We always carry out a DPIA if we plan to:
    - ☐ Use systematic and extensive profiling or automated decision-making to make significant decisions about people.
    - ☐ Process special category data or criminal offence data on a large scale.
    - ☐ Systematically monitor a publicly accessible place on a large scale.
    - ☐ Use new technologies.
    - ☐ Use profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit.
    - ☐ Carry out profiling on a large scale.
    - ☐ Process biometric or genetic data.
    - ☐ Combine, compare or match data from multiple sources.
    - ☐ Process personal data without providing a privacy notice directly to the individual.

- ☐ Process personal data in a way which involves tracking individuals' online or offline location or behaviour.
- ☐ Process children's personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them.
- ☐ Process personal data which could result in a risk of physical harm in the event of a security breach.

☐ We consider whether to do a DPIA if we plan to carry out any other:

- ☐ Evaluation or scoring.
- ☐ Automated decision-making with significant effects.
- ☐ Systematic monitoring.
- ☐ Processing of sensitive data or data of a highly personal nature.
- ☐ Processing on a large scale.
- ☐ Processing of data concerning vulnerable data subjects.
- ☐ Innovative technological or organisational solutions.
- ☐ Processing involving preventing data subjects from exercising a right or using a service or contract.

☐ If we decide not to carry out a DPIA, we document our reasons.

☐ We consider carrying out a DPIA in any major project involving the use of personal data.

☐ We carry out a new DPIA if there is a change to the nature, scope, context or purposes of our processing.

DPIA process checklist

☐ We describe the nature, scope, context and purposes of the processing.

☐ We ask our data processors to help us understand and document their processing activities and identify any associated risks.

☐ We consider how best to consult individuals (or their representatives) and other relevant stakeholders.

- ☐ We ask for the advice of our data protection officer.

- ☐ We check that the processing is necessary for and proportionate to our purposes, and describe how we will ensure data protection compliance.

- ☐ We do an objective assessment of the likelihood and severity of any risks to individuals' rights and interests.

- ☐ We identify measures we can put in place to eliminate or reduce high risks.

- ☐ We record the outcome of the DPIA, including any difference of opinion with our DPO or individuals consulted.

- ☐ We implement the measures we identified, and integrate them into our project plan.

- ☐ We consult the ICO before processing, if we cannot mitigate high risks.

- ☐ We keep our DPIAs under review and revisit them when necessary.