Accountability and governance

Data Protection Impact Assessments (DPIAs)

ico.
Information Commissioner's Office

Data protection impact assessments

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 processing that is **likely to result in a high risk** to individuals. This includes some specified types of processing. 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.

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
- ☐ 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.

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

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

☐ 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 our decision-making in 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.

In brief

- What's new under the GDPR?
- What is a DPIA?
- When do we need a DPIA?
- How do we carry out a DPIA?
- Do we need to consult the ICO?

What's new under the GDPR?

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.

What is a DPIA?

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.

When do we need a DPIA?

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;

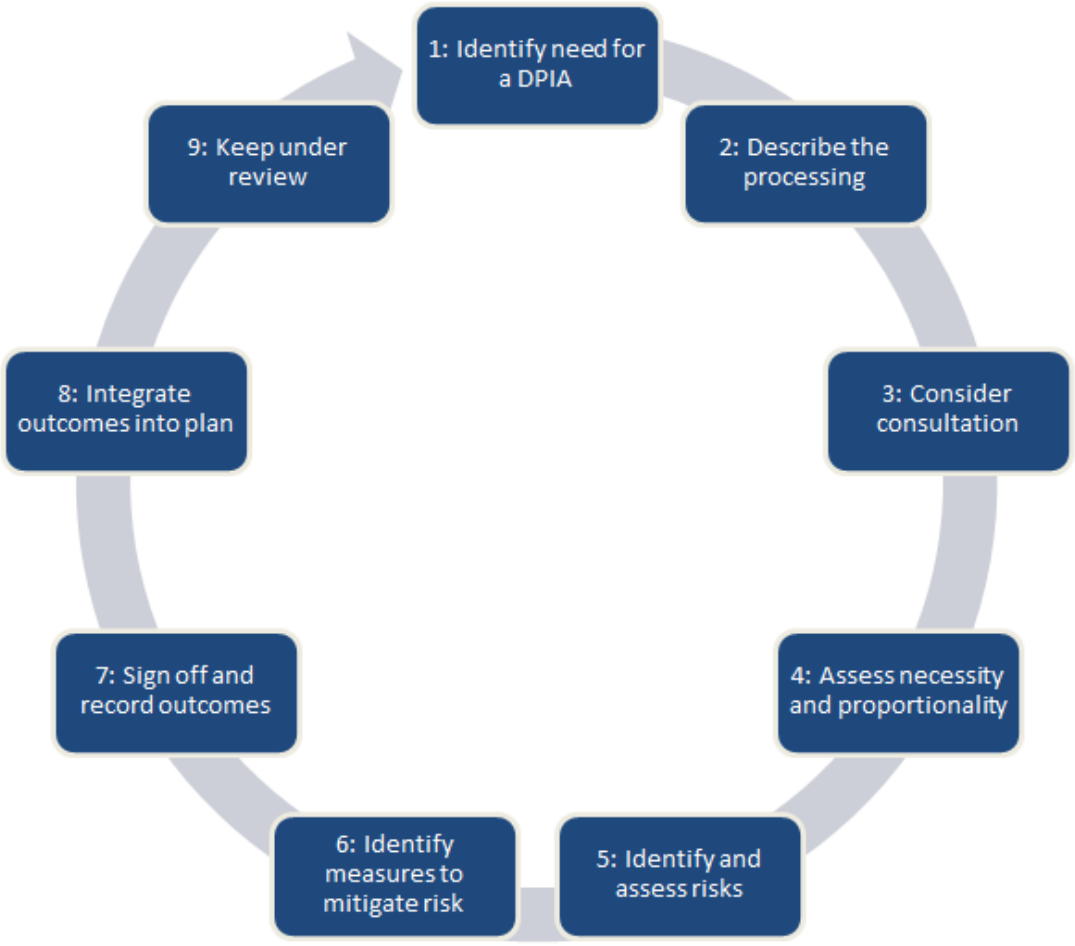
- profile individuals on a large scale;
- process biometric data;
- process genetic data;
- match data or combine datasets from different sources;
- collect personal data from a source other than the individual without providing them with a privacy notice (‘invisible processing’);
- track individuals’ 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. You can use or adapt the checklists to help you carry out this screening exercise.

How do we carry out a DPIA?

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.

Although publishing a DPIA is not a requirement of GDPR, you should actively consider the benefits of publication. As well as demonstrating compliance, publication can help engender trust and confidence. We would therefore recommend that you publish your DPIAs, were possible, removing sensitive details if necessary.

Do we need to consult the ICO?

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.

Further Reading

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

Further reading – ICO guidance

We have published more detailed guidance on DPIAs.

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 10
What’s new under the GDPR? 12
What is a DPIA? 14
When do we need to do a DPIA? 18
How do we do a DPIA? 29
Do we need to consult the ICO? 39
Examples of processing ‘likely to result in high risk’ 42

About this detailed guidance

This guidance discusses Data Protection Impact Assessments (DPIAs) in detail. Read it if you have detailed questions not answered in the Guide, or if you need a deeper understanding to help you understand or complete a DPIA in practice. DPOs and those with specific data protection responsibilities in larger organisations are likely to find it useful.

The guidance has been revised to adopt the European Data Protection Board's 22/2018 opinion on the ICO's list of processing operations subject to the requirement of conducting a DPIA.

If you haven't yet read DPIAs in brief in the Guide to GDPR, you should read that first. It sets out the key points you need to know, along with practical checklists to help you comply.

Contents

What's new?

Is this a new obligation?

What should we do if we already carry out DPIAs?

What should we do it we don't already carry out DPIAs?

What is a DPIA?

What is a DPIA?

Why are DPIAs important?

How are DPIAs used?

What kind of 'risk' do they assess?

When do we need to do a DPIA?

What is the general rule?

What does 'high risk' mean?

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

What types of processing automatically require a DPIA?

What other factors might indicate likely high risk?

What does the ICO consider likely to result in high risk?

What does 'innovative technologies' mean?

What does 'systematic and extensive'

How do we carry out a DPIA?

What are the key elements of a DPIA process?

Is there a template we can use?

Who should do the DPIA?

What is the role of the DPO?

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

Step 2: How do we describe the processing?

Step 3: Do we need to consult individuals?

Step 3: Do we need to consult anyone else?

Step 4: How do we assess necessity and proportionality?

mean?

What does ‘significantly affect’ mean?

What does ‘invisible processing’ mean?

What does ‘vulnerable individual’ mean?

What does ‘large scale’ mean?

Are there any exemptions?

Step 5: How do we identify and assess risks?

Step 6: How do we identify mitigating measures?

Step 7: How do we conclude our DPIA?

What happens next?

Do we need to consult the ICO?

When do we need to consult the ICO?

How do we consult the ICO?

What happens next?

What happens if we do not accept your DPIA?

How is our DPIA assessed?

How long does it take?

What are the possible outcomes?

Can we appeal?

Examples of processing ‘likely to result in high risk’

List of examples of processing 'likely to result in high risk'

What's new under the GDPR?

In detail

- Is this a new obligation?
- What should we do if we already carry out DPIAs?
- What should we do if we don't already carry out DPIAS?

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.

Further Reading

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

What should we do if we already carry out PIAs?

Privacy impact assessments (PIAs) have been used for many 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 PIA code under DPA 1998, the new process will be very familiar.

However, you will need to review and 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 should also seek the views of people whose data you intend to process, or their representatives, where appropriate.
- 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 you understand DPIA requirements and embed them into your business practices. If you are likely to do many DPIAs, consider using this guidance as a starting point to design a bespoke DPIA process to meet your specific needs and fit in with your existing practices.

You should also review your existing processing operations to identify whether you already do anything that would be considered likely to result in high risk under the GDPR. If so, are you confident you have already adequately assessed and mitigated your project's risks? 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 existing 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 the nature, scope, context or purposes of the processing have changed significantly since that previous assessment.

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

Further Reading

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

Further reading - European Data Protection Board

WP29 produced guidelines on data protection impact assessments, which have been endorsed by the EDPB.

What is a DPIA?

In detail

- What is a DPIA?
- Why are DPIAs important?
- How are DPIAs used?
- What kind of 'risk' do they assess?

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.

Further Reading

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

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, including certain specified types of processing that are likely to result in a high risk to the rights and freedoms of individuals. Under GDPR, failure to carry out a DPIA when required may leave you open to enforcement action, including a fine of up to €10 million, or 2% global annual turnover if higher.

By considering the risks related to your intended processing before you begin, you also support compliance with another general obligation under GDPR: data protection by design and default.

Article 25 is clear that:

> “the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures… and … integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.”

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

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.

Further Reading

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

In more detail – ICO guidance

Read the ICO guidance on the Article 25 requirement to implement data protection by design and default.

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:

> "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.

Further Reading

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

Further reading - European Data Protection Board

WP29 produced guidelines on data protection impact assessments, which have been endorsed by the EDPB.

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:

> "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.

Further Reading

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

Further reading - European Data Protection Board

WP29 produced guidelines on data protection impact assessments, which have been endorsed by the EDPB.

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 detail

- What is the general rule?
- What does ‘high risk’ mean?
- What does ‘likely to result in a high risk’ mean?
- What types of processing automatically require a DPIA?
- What other factors might indicate likely high risk?
- What does the ICO consider likely to result in high risk?
- What does ‘innovative technologies’ mean?
- What does ‘systematic and extensive’ mean?
- What does ‘significantly affect’ mean?
- What does ‘invisible processing’ mean?
- What does ‘vulnerable individual’ mean?
- What does ‘large scale’ mean?
- Are there any exemptions?

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:

> “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**:

> "(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**:

> "(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**:

> “(c) a systematic monitoring of a publicly accessible area on a large scale.”

What other factors might indicate likely high risk?

The Article 29 working party of EU data protection authorities (WP29) 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.

For more guidance on these factors, read the WP29 guidelines (WP248). They give background on the reasoning for the high-risk indicators, and examples of processing likely to result in high risk.

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.

Further reading - European Data Protection Board

WP29 produced guidelines on data protection impact assessments, which have been endorsed by the EDPB.

Further Reading

Relevant provisions in the GDPR - See Recitals 89 and 91
External link

What does the ICO consider likely to result in high risk?

The ICO is required by Article 35(4) to publish a list of processing operations that require a DPIA. This list complements and further specifies the criteria referred to in the European guidelines. Some of these operations require a DPIA automatically, and some only when they occur in combination with one of the other items, or any of the criteria in the European Guidelines referred to above:

1. **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.
2. **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.
3. **Large-scale profiling:** any profiling of individuals on a large scale.
4. **Biometrics:** any processing of biometric data. A DPIA is required where this processing is combined with any of the criteria from the European guidelines.
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. A DPIA is required where this processing is combined with any of the criteria from the European guidelines.
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. A DPIA is required where this processing is combined with any of the criteria from the European guidelines.
8. **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.
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.
0. **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.

In more detail – ICO guidance

For indicative examples of operations that require a DPIA, and further detail on which criteria are high risk in combination with others, read our list of processing operations 'likely to result in high risk'.

Further Reading

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

What does ‘innovative technologies’ mean?

Recital 91 says innovative technology concerns new developments in technological knowledge in the world at large, rather than technology that is new to you, and its use can trigger the need to carry out a DPIA. This is because using such technology can involve novel forms of data collection and use, possibly with a high risk to individuals’ rights and freedoms. The personal and social consequences of deploying a new technology may be unknown, and a DPIA can help the controller to understand a control such risks.

Examples of processing using innovative technology include:

- artificial intelligence, machine learning and deep learning;
- connected and autonomous vehicles;
- intelligent transport systems;
- smart technologies (including wearables);
- market research involving neuro-measurement (e.g. emotional response analysis and brain activity);
- some ‘internet of things’ applications, depending on the specific circumstances of the processing.

It is not just cutting-edge technology that might be classed as innovative. If a controller implements existing technology in a new way, this could result in high risks that, unless a DPIA is done, may not be identified and dealt with. For example, doing a DPIA as part of a project to design and deploy a large-scale database system that processes customer details could:

- help in deciding what proportionate security measures should be implemented (e.g. protective monitoring);
- and act as a reminder that GDPR-compliant contracts need to be in place with any processors.

The ICO list of high-risk processing operations requires a DPIA if your processing involves innovative technology in combination with another criterion from the European guidelines (e.g. evaluation or scoring, or sensitive data).

However, in some cases you may decide that your intended use of innovative technology requires a DPIA without any other factors. As controller, if no mandatory obligation applies, you are responsible for assessing whether your intended processing is ‘likely to result in high risk’.

Further reading

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

Further Reading

Relevant provisions in the GDPR - See Articles 35(1) and Recitals 89 and 91
External link

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 – European Data Protection Board

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

Further Reading

Relevant provisions in the GDPR - See Articles 35(3)(a) and (c) and Recital 91
External link

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 significantly affect their circumstances, behaviour or choices.

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 significantly affect more vulnerable people, such as children.

In more detail – ICO guidance

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 regarding children and their personal data.

Further reading – European Data Protection Board

Read the WP29 Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679 (WP251). They contain guidance on legal and similarly significant effects.

Further Reading

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

What does 'invisible processing' mean?

'Invisible processing' occurs when you obtain personal data from somewhere other than directly from the individual themselves, and you don't provide them with the privacy information required by Article 14. The processing is 'invisible' because the individual is unaware that you are collecting and using their personal data, even if you publish a privacy notice on your website.

This processing results in a risk to the individual's interests as they cannot exercise any control over your use of their data. In particular, they are unable to use their data protection rights if they are unaware of the processing. This is true even if the processing itself is unlikely to have any negative effect.

You may also be at risk of breaching the fairness and transparency requirements of the first data protection principle if the processing, or any outcome from it, may not be reasonably foreseen by the individual.

For these reasons, processing in this way is only permitted by the GDPR in limited circumstances. These include where to provide the privacy information proves **impossible** or would involve a **disproportionate effort**.

Circumstances when it is impossible to provide privacy will only arise rarely, for example where you have no contact details for individuals and have no reasonable means of obtaining them.

It is important that you can demonstrate compliance with individuals' right to be informed. So, if you are proposing processing operations that involve the use of data obtained from third parties, you must first carefully consider whether you can provide privacy information to the individuals. If you intend to rely on the exception for disproportionate effort, you must be able to justify this, and you must take other measures to protect people's rights. In particular, you must still publish your privacy information, and carry out a DPIA.

Your DPIA will help you assess and demonstrate whether you are taking a proportionate approach. It will help you consider how best to mitigate the impact on individuals' ability to exercise control over their data, and whether you can take other measures to support the exercise of their rights. It will also help you demonstrate how you comply with fairness and transparency requirements.

In more detail – ICO guidance

Read the ICO guidance on the right to be informed, which includes a section on disproportionate effort and other exceptions and exemptions.

Further reading – European Data Protection Board

See the WP29 guidelines on Transparency, which have been endorsed by the EDPB.

Further Reading

Relevant provisions in the GDPR - See Articles 14(1), (2) and (5) and Recitals 60, 61 and 62
External link

What does 'vulnerable individual' mean?

Individuals can be vulnerable where circumstances may restrict their ability to freely consent or object to the processing of their personal data, or to understand its implications.

Most obviously, children are regarded as vulnerable to the processing of their personal data since they may be less able to understand how their data is being used, anticipate how this might affect them, and protect themselves against any unwanted consequences. This can also be true of other vulnerable sections of the population such as elderly people, or those with certain disabilities.

Even if the individuals are not part of a group you might automatically consider vulnerable, an imbalance of power in their relationship with you can cause vulnerability for data protection purposes if they believe that they will be disadvantaged if the processing doesn't go ahead.

One group who may count as vulnerable in this sense are employees. The European guidelines on DPIAs (WP248) explain why employees could be considered vulnerable data subjects where a power imbalance means they cannot easily consent or object to the processing of their data by an employer. This type of vulnerability could also arise due to an individual's financial situation (e.g. credit rating) or the specific context of the processing (e.g. patients receiving medical care).

Processing the data of individuals who may be deemed vulnerable is one of the criteria in European guidelines for processing likely to result in high risk. If you think your processing will involve vulnerable individuals, then a DPIA will be required should any of the other criteria, or operations on our list, be engaged.

Example

A sales firm provides company cars for their employees, and intends to deploy vehicles with location-tracking features, allowing managers to monitor the movement and whereabouts of their

employees at all times. Employees are also permitted to use the vehicles for their private purposes outside working hours.

The processing intends to track each individual's geolocation, in a context where they are vulnerable to a power imbalance with the controller. So this engages the requirement for a DPIA to identify and mitigate the risks to the employees' rights and freedoms.

Further Reading

Relevant provisions in the GDPR - See Articles 35(3) and Recitals 38, 75 and 91
External link

In more detail – ICO guidance

Read our guidance on children and the GDPR for more on consent and the extra protections for children.

Further reading – European Data Protection Board

WP29 produced guidelines on data protection impact assessments, which have been endorsed by the EDPB.

Read the WP29 Opinion 2/2017 on data processing at work for more on the processing of personal data in an employment context.

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.

Further Reading

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

Further reading – European Data Protection Board

WP29 produced guidelines on data protection impact assessments, which have been endorsed by the EDPB.

Also read the WP29 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 derived from specific legislation, such as Digital Economy Act 2017; or
  - 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. So in the absence of any clear and authoritative statement on whether such an assessment was done, we recommend you err on the side of caution and do 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.

Further Reading

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

Further reading – European Data Protection Board

WP29 produced guidelines on data protection impact assessments, which have been endorsed by the EDPB.

How do we do a DPIA?

In detail

- What are the key elements of a DPIA process?
- Is there a template we can use?
- Who should do the DPIA?
- What is the role of the DPO?
- Step 1: How do we decide whether to do a DPIA?
- Step 2: How do we describe the processing?
- Step 3: Do we need to consult individuals?
- Step 3: Do we need to consult anyone else?
- Step 4: How do we assess necessity and proportionality?
- Step 5: How do we identify and assess risks?
- Step 6: How do we identifying mitigating measures?
- Step 7: How do we conclude our DPIA?
- What happens next?

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

After sign-off you should integrate the outcomes from your DPIA back into your project plan, and keep your DPIA under review. Throughout this process, you should consult individuals and other stakeholders as needed.

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.

Further Reading

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

Further reading

WP29 produced guidelines on data protection impact assessments, which have been endorsed by the EDPB. Annex 2 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 make your own to suit your needs, or use an existing project-management method, as long as it covers all the key elements of the process. If you are making your own template, you may 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 in your organisation, and who signs them off. You can outsource your DPIA, but you remain responsible for it. If you have a Data Protection Officer (DPO), you must ask for their advice on your DPIA, and document it as part of the process.

You may want to ask a processor to carry out a DPIA on your behalf if they do the relevant processing operation, but again you remain responsible for it.

Who should be involved in the DPIA?

As well as the business area or individual who is leading on the project or process requiring the DPIA, you should also involve:

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

Further reading

WP29 produced guidelines on data protection impact assessments, which have been endorsed by the EDPB.

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 DPIA's ongoing performance, including how well you have implemented your planned actions to address the risks.

Under Article 39 of GDPR, DPOs have specific tasks regarding DPIAs. This is why you must ensure that any responsibilities you give a DPO for your DPIA do not conflict with their ability to complete these tasks in an independent manner, as required by Recital 97.

Further Reading

> Relevant provisions in the GDPR - See Articles 35(2)and 39(1)(c)
> External link

In more detail – ICO guidance

Read our guidance on data protection officers for more detail on the tasks for DPOs regarding DPIAs.

Further reading – European Data Protection Board

Read the WP29 Guidelines on Data Protection Officers (WP243).

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

Ask your DPO for advice. If you have any major project that involves the use of personal data, it is good practice to do 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 that automatically require a DPIA. If not, you need to screen for other factors that may indicate it is a type of processing that is likely to result in high risk, such as processing the data of vulnerable individuals.

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

If you do this screening and decide a DPIA is not needed, you should document your decision and the reasons for it, including your DPO's advice. This does not have to be a burdensome paperwork exercise. It just needs to help you demonstrate 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;
- how far individuals have control over their data;
- how far individuals are likely to expect the processing;

- whether these individuals 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;
- in due course, whether you comply with any GDPR codes of conduct (once any have been approved under Article 40) or GDPR certification schemes;and
- 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.

Further Reading

> Relevant provisions in the GDPR - See Article 35(7)(a) and Recitals 84, 90 and 94
> External link

Step 3: Do we need to consult individuals?

You should seek and document 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 this is not appropriate, you should record this decision as part of your DPIA, with a clear explanation. For example, you may 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 market research with a certain demographic or contacting relevant campaign or consumer groups for their views.

If your DPIA decision differs from the views of individuals, you need to document your reasons for disregarding their views.

Further Reading

> Relevant provisions in the GDPR - See Article 35(9)
> External link

Further reading

WP29 produced guidelines on data protection impact assessments, which have been endorsed by the EDPB.

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.

Further Reading

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

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?

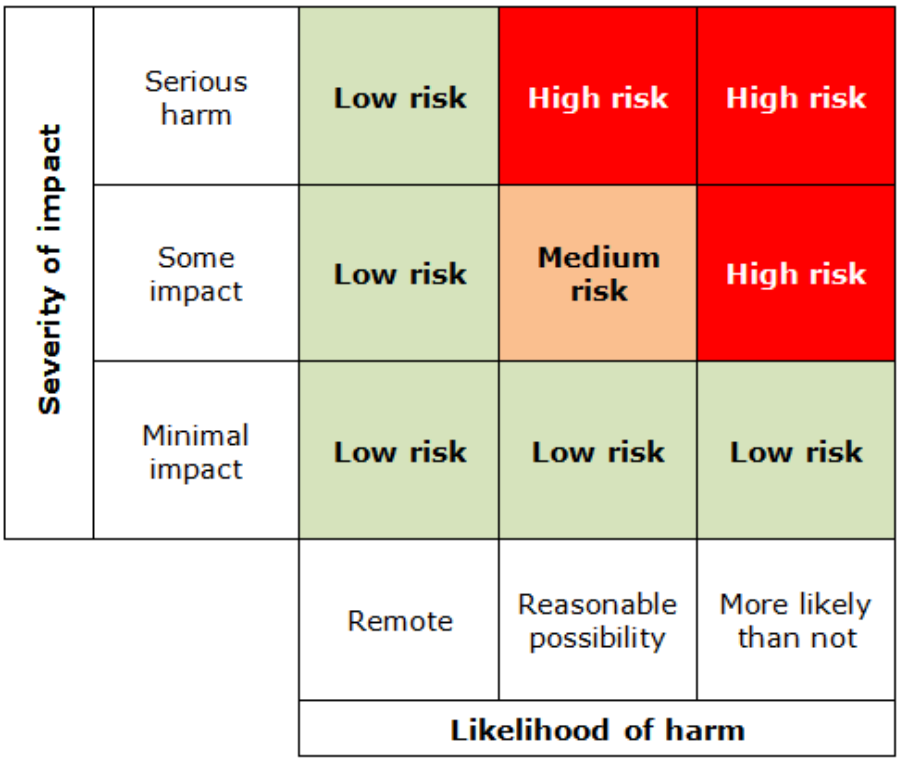
Consider the potential impact on individuals and any harm or damage your processing may cause – whether physical, emotional or material. In particular, look at whether the processing could contribute to:

- 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;
- re-identification 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 to 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 may still count as high risk.

You must make an objective assessment of the risks. It is helpful to use a structured matrix to think about likelihood and severity of risks:



The above matrix shows a structured way to assess risk. Your organisation may use a different method you can adapt for the same purpose.

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

Further Reading

Relevant provisions in the GDPR - See Articles 35(7)(c) and Recitals 76 and 90
External link

Step 6: How do we identify mitigating measures?

Against each risk identified, record its source. 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;
- 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 seek and document DPO advice 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 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 must consult the ICO before you go ahead with the processing. See the next section for more information on this consultation process.

To aid transparency and accountability, it is good practice to publish your DPIA. This could help foster trust in your processing activities, and improve individuals' ability to exercise their rights. If you are concerned that publication may 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.

When considering publishing DPIAs, public authorities should think about their wider transparency obligations, such as complying with the Freedom of Information Act. Before GDPR, many public authorities included privacy impact assessments in their definition documents for publication schemes.

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

Further Reading

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

Further reading

WP29 produced guidelines on data protection impact assessments, which have been endorsed by the EDPB.

Do we need to consult the ICO?

In detail

- When do we need to consult the ICO?
- How do we consult the ICO?
- What happens next?
- What happens if we do not accept your DPIA?
- How is our DPIA assessed?
- How long does it take?
- What are the possible outcomes?
- Can we appeal?

When do we need to consult the ICO?

If you have carried out a DPIA that identifies a high risk and you cannot do anything to reduce it, prior consultation with the ICO is required under GDPR. You cannot go ahead with the processing until you have consulted us.

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

Further Reading

> Relevant provisions in the GPDR - See Article 36(1) and Recital 94
> External link

Further reading - European Data Protection Board

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?

Send us a copy of your submission. 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 (if you have one); and
- a copy of the DPIA.

Further Reading

Key provisions in the GDPR - See Article 36(3)
External link

What happens next?

When we receive your DPIA, we will send you an acknowledgement and check we have all the information we need.

We will write to you to within 10 days to let you know if we have accepted your DPIA for prior consultation. We will explain our reasoning.

You may not hear from us again until we provide our written advice. If we have further queries, we may make contact to arrange a telephone call or meeting with you.

Further Reading

Relevant provisions in the GDPR - See Article 36(2)
External link

What happens if we do not accept your DPIA?

We may wish to discuss your proposed processing with you, even if your DPIA does not meet the criteria for prior consultation. If so, we will explain to you how we would like to engage with you.

How is your DPIA assessed?

If we accept your DPIA, we don't just look at the risks you documented. We consider all of your submission – your DPIA documentation and any further information you provided – along with any prior contact you may have had with our office.

We seek to understand in detail the context and nature of the processing you are proposing, including any controller-processor relationships. We will also assess the extent to which you have evidenced compliance with the Data Protection Principles.

To do this effectively, we may need to ask you to give us more information.

How long does it take?

Where we provide advice under the prior consultation process, we will get back to you within eight weeks of receipt of your DPIA. In complex cases, we can 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. We will explain our reasons.

If we need to ask for more information, we cannot continue our assessment until you provide it. To prevent further delay, please ensure you include any documents your assessment refers to, such as privacy notices.

If your intended processing operation would affect data subjects in EU member states, we may be required to co-operate with other data protection authorities before providing our written advice, in line with Chapter VII GDPR. This may mean your case cannot be resolved in 14 weeks. We will notify you if this occurs and keep you updated.

Further Reading

> Relevant provisions in the GDPR - See Article 36(2)
> External link

What are the possible outcomes?

We may come to the view, based on your DPIA, that risks have been sufficiently identified and mitigated, and that you may proceed with the processing.

Our written response could be limited to advice on how you can further mitigate identified risks before you proceed with your processing.

In some circumstances, we may also issue an official warning, a new corrective power under GDPR, alongside any advice we provide. We will issue warnings where we are concerned that your intended processing is likely to contravene GDPR. Any warning will explain the reasons for our concerns, and the steps we recommend you take to avoid any contravention.

If we have more significant concerns, we may impose a limitation or ban on your intended processing.

In any outcome, our written response to you will make clear what you may and may not do.

Further Reading

> Key provisions in the GDPR - See Articles 36(2) and 58
> External link

Can we appeal?

Warnings are not subject to appeal, but you may seek judicial review if you disagree with the way we made the decision.

You can seek a review of other corrective measures (such as limitations or bans on processing) by appeal to the First Tier Tribunal.

More information on appeals against the Information Commissioner can be found here.

Examples of processing ‘likely to result in high risk’

The following list details processing operations for which the ICO requires you to complete a DPIA as they are ‘likely to result in high risk’. It is based on guidelines adopted by the European Data Protection Board (EDPB) on DPIAs (WP248rev01). Our list therefore complements and further specifies these guidelines.

For illustration, we have also included examples of existing areas of application. These should not be taken as definitive or exhaustive. In any event, this list does not affect your overriding obligation in Article 35(1), which is to assess any proposed processing operation against the requirement to complete DPIAs. The ICO also considers it best practice to do a DPIA, whether or not the processing is likely to result in a high risk.

Type of processing operation(s) requiring a DPIA	Description	Non-exhaustive examples of existing areas of application
Innovative technology	Processing involving the use of new technologies, or the novel application of existing technologies (including AI). A DPIA is required for any intended processing operation(s) involving innovative use of technologies (or applying new technological and/or organisational solutions) when combined with any other criterion from WP248rev01.	• Artificial intelligence, machine learning and deep learning • Connected and autonomous vehicles • Intelligent transport systems • Smart technologies (including wearables) • Market research involving neuro-measurement (i.e. emotional response analysis and brain activity) • Some IoT applications, depending on the specific circumstances of the processing
Denial of service	Decisions about an individual’s access to a product, service, opportunity or benefit which are based to any extent on automated decision-making (including profiling) or involves the processing of special- category data.	• Credit checks • Mortgage or insurance applications • Other pre-check processes related to contracts (i.e. smartphones)
Large-scale profiling	Any profiling of individuals on a large scale	• Data processed by Smart Meters or IoT applications • Hardware/software offering fitness/lifestyle monitoring • Social-media networks • Application of AI to existing

		process
Biometric data	Any processing of biometric data for the purpose of uniquely identifying an individual. A DPIA is required for any intended processing operation(s) involving biometric data for the purpose of uniquely identifying an individual, when combined with any other criterion from WP248rev01	• Facial recognition systems • Workplace access systems/identity verification • Access control/identity verification for hardware/applications (including voice recognition/fingerprint /facial recognition)
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 for any intended processing operation(s) involving genetic data when combined with any other criterion from WP248rev01	• Medical diagnosis • DNA testing • Medical research
Data matching	Combining, comparing or matching personal data obtained from multiple sources	• Fraud prevention • Direct marketing • Monitoring personal use/uptake of statutory services or benefits • Federated identity assurance services
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 (as provided by Article 14.5(b). A DPIA is required for any intended processing operation(s) involving where the controller is relying on Article 14.5(b) when combined with any other criterion from WP248rev01	• List brokering • Direct marketing • Online tracking by third parties • Online advertising • Data aggregation/data aggregation platforms • Re-use of publicly available data
Tracking	Processing which involves tracking an individual's geolocation or behaviour, including but not limited	• Social networks, software applications • Hardware/software offering

	to the online environment. A DPIA is required for any intended processing operation involving geolocation data when combined with any other criterion from WP248rev01	fitness/lifestyle/health monitoring • IoT devices, applications and platforms • Online advertising • Web and cross-device tracking • Data aggregation / data aggregation platforms • Eye tracking • Data processing at the workplace • Data processing in the context of home and remote working • Processing location data of employees • Loyalty schemes • Tracing services (tele-matching, tele-appending) • Wealth profiling – identification of high net-worth individuals for the purposes of direct marketing
Targeting of children/other vulnerable individuals for marketing, profiling for auto decision making or the offer of online services	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.	• Connected toys • Social networks
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.	• Whistleblowing/complaint procedures • Social care records

About this detailed guidance 46
What is a DPIA? 49
When do we need to do a DPIA? 54
How do we do a DPIA? 65
Do we need to consult the ICO? 75
Examples of processing ‘likely to result in high risk’ 78

About this detailed guidance

The Brexit transition period ended on 31 December 2020. The GDPR has been retained in UK law as the UK GDPR, and will continue to be read alongside the Data Protection Act 2018, with technical amendments to ensure it can function in UK law. If you transfer or receive data from overseas please visit our End of Transition and International Transfers pages. You should make sure you can identify any data you collected before the end of 2020 about people outside the UK, for further information, see our Q&A on Legacy Data.

On 01 January, there will not be any significant change to the UK data protection regime, or to the criteria that compel DPIAs. This guidance draws on European resources which we still consider to be relevant, and so these resources remain part of our DPIA guidance.

We will keep this guidance under review and update it as and when any aspect of your obligations or our approach changes. Please continue to monitor our website for updates.

This guidance discusses Data Protection Impact Assessments (DPIAs) in detail. Read it if you have detailed questions not answered in the Guide, or if you need a deeper understanding to help you understand or complete a DPIA in practice. DPOs and those with specific data protection responsibilities in larger organisations are likely to find it useful.

The guidance has been revised to adopt the European Data Protection Board's 22/2018 opinion on the ICO's list of processing operations subject to the requirement of conducting a DPIA.

If you haven't yet read DPIAs in brief in the Guide to GDPR, you should read that first. It sets out the key points you need to know, along with practical checklists to help you comply.

Contents

What is a DPIA?

What is a DPIA?

Why are DPIAs important?

How are DPIAs used?

What kind of 'risk' do they assess?

When do we need to do a DPIA?

What is the general rule?

What does 'high risk' mean?

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

What types of processing automatically require a DPIA?

What other factors might indicate likely high risk?

What does the ICO consider likely to result in high risk?

What does ‘innovative technologies’ mean?

What does ‘systematic and extensive’ mean?

What does ‘significantly affect’ mean?

What does ‘invisible processing’ mean?

What does ‘vulnerable individual’ mean?

What does ‘large scale’ mean?

Are there any exemptions?

How do we carry out a DPIA?

What are the key elements of a DPIA process?

Is there a template we can use?

Who should do the DPIA?

What is the role of the DPO?

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

Step 2: How do we describe the processing?

Step 3: Do we need to consult individuals?

Step 3: Do we need to consult anyone else?

Step 4: How do we assess necessity and proportionality?

Step 5: How do we identify and assess risks?

Step 6: How do we identify mitigating measures?

Step 7: How do we conclude our DPIA?

What happens next?

Do we need to consult the ICO?

When do we need to consult the ICO?

How do we consult the ICO?

What happens next?

What happens if we do not accept your DPIA?

How is our DPIA assessed?

How long does it take?

What are the possible outcomes?

Can we appeal?

Examples of processing ‘likely to result in high risk’

List of examples of processing 'likely to result in high risk'

What is a DPIA?

In detail

- What is a DPIA?
- Why are DPIAs important?
- How are DPIAs used?
- What kind of 'risk' do they assess?

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 UK 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.

Further Reading

> Relevant provisions in the UK GDPR - See Articles 35(1) and 35(7) and Recitals 84 and 90
> External link

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, including certain specified types of processing that are likely to result in a high risk to the rights and freedoms of individuals. Under UK GDPR, failure to carry out a DPIA when required may leave you open to enforcement action, including a fine of up to £8.7 million, or 2% global annual turnover if higher.

By considering the risks related to your intended processing before you begin, you also support compliance with another general obligation under UK GDPR: data protection by design and default.

Article 25 is clear that:

> “the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures… and … integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.”

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

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.

Further Reading

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

In more detail – ICO guidance

Read the ICO guidance on the Article 25 requirement to implement data protection by design and default.

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 UK GDPR is clear that:

> "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.

Further Reading

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

Further reading - European Data Protection Board

WP29 produced guidelines on data protection impact assessments, which have been endorsed by the EDPB.

What kind of 'risk' do they assess?

There is no explicit definition of 'risk' in the UK 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:

> "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 UK 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.

Further Reading

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

Further reading - European Data Protection Board

WP29 produced guidelines on data protection impact assessments, which have been endorsed by the EDPB.

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 detail

- What is the general rule?
- What does ‘high risk’ mean?
- What does ‘likely to result in a high risk’ mean?
- What types of processing automatically require a DPIA?
- What other factors might indicate likely high risk?
- What does the ICO consider likely to result in high risk?
- What does ‘innovative technologies’ mean?
- What does ‘systematic and extensive’ mean?
- What does ‘significantly affect’ mean?
- What does ‘invisible processing’ mean?
- What does ‘vulnerable individual’ mean?
- What does ‘large scale’ mean?
- Are there any exemptions?

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:

> “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 UK 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 UK 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 UK 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**:

> "(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**:

> "(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**:

> “(c) a systematic monitoring of a publicly accessible area on a large scale.”

What other factors might indicate likely high risk?

The Article 29 working party of EU data protection authorities (WP29) 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.

For more guidance on these factors, read the WP29 guidelines (WP248). They give background on the reasoning for the high-risk indicators, and examples of processing likely to result in high risk.

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.

Further reading - European Data Protection Board

WP29 produced guidelines on data protection impact assessments, which have been endorsed by the EDPB.

Further Reading

Relevant provisions in the UK GDPR - See Recitals 89 and 91
External link

What does the ICO consider likely to result in high risk?

The ICO is required by Article 35(4) to publish a list of processing operations that require a DPIA. This list complements and further specifies the criteria referred to in the European guidelines. Some of these operations require a DPIA automatically, and some only when they occur in combination with one of the other items, or any of the criteria in the European Guidelines referred to above:

1. **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.
2. **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.
3. **Large-scale profiling:** any profiling of individuals on a large scale.
4. **Biometrics:** any processing of biometric data. A DPIA is required where this processing is combined with any of the criteria from the European guidelines.
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. A DPIA is required where this processing is combined with any of the criteria from the European guidelines.
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. A DPIA is required where this processing is combined with any of the criteria from the European guidelines.
8. **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.
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.

In more detail – ICO guidance

For indicative examples of operations that require a DPIA, and further detail on which criteria are high risk in combination with others, read our list of processing operations 'likely to result in high risk'.

Further Reading

Relevant provisions in the UK GDPR - See Articles 35(3) and 35(4)
External link

What does ‘innovative technologies’ mean?

Recital 91 says innovative technology concerns new developments in technological knowledge in the world at large, rather than technology that is new to you, and its use can trigger the need to carry out a DPIA. This is because using such technology can involve novel forms of data collection and use, possibly with a high risk to individuals’ rights and freedoms. The personal and social consequences of deploying a new technology may be unknown, and a DPIA can help the controller to understand a control such risks.

Examples of processing using innovative technology include:

- artificial intelligence, machine learning and deep learning;
- connected and autonomous vehicles;
- intelligent transport systems;
- smart technologies (including wearables);
- market research involving neuro-measurement (e.g. emotional response analysis and brain activity);
- some ‘internet of things’ applications, depending on the specific circumstances of the processing.

It is not just cutting-edge technology that might be classed as innovative. If a controller implements existing technology in a new way, this could result in high risks that, unless a DPIA is done, may not be identified and dealt with. For example, doing a DPIA as part of a project to design and deploy a large-scale database system that processes customer details could:

- help in deciding what proportionate security measures should be implemented (e.g. protective monitoring);
- and act as a reminder that UK GDPR-compliant contracts need to be in place with any processors.

The ICO list of high-risk processing operations requires a DPIA if your processing involves innovative technology in combination with another criterion from the European guidelines (e.g. evaluation or scoring, or sensitive data).

However, in some cases you may decide that your intended use of innovative technology requires a DPIA without any other factors. As controller, if no mandatory obligation applies, you are responsible for assessing whether your intended processing is ‘likely to result in high risk’.

Further reading

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

Further Reading

Relevant provisions in the UK GDPR - See Articles 35(1) and Recitals 89 and 91
External link

What does ‘systematic and extensive’ mean?

Again, the UK 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 – European Data Protection Board

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

Further Reading

Relevant provisions in the UK GDPR - See Articles 35(3)(a) and (c) and Recital 91
External link

What does 'significantly affect' mean?

The UK 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 significantly affect their circumstances, behaviour or choices.

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 significantly affect more vulnerable people, such as children.

In more detail – ICO guidance

Read our guidance on profiling and automated decision-making for more on legal and similarly significant effects.

Read our guidance on children and the UK GDPR for more on significant effects specifically regarding children and their personal data.

Further reading – European Data Protection Board

Read the WP29 Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679 (WP251). They contain guidance on legal and similarly significant effects.

Further Reading

Relevant provisions in the UK GDPR - See Article 35(3)(a) and Recital 91
External link

What does 'invisible processing' mean?

'Invisible processing' occurs when you obtain personal data from somewhere other than directly from the individual themselves, and you don't provide them with the privacy information required by Article 14. The processing is 'invisible' because the individual is unaware that you are collecting and using their personal data, even if you publish a privacy notice on your website.

This processing results in a risk to the individual's interests as they cannot exercise any control over your use of their data. In particular, they are unable to use their data protection rights if they are unaware of the processing. This is true even if the processing itself is unlikely to have any negative effect.

You may also be at risk of breaching the fairness and transparency requirements of the first data protection principle if the processing, or any outcome from it, may not be reasonably foreseen by the individual.

For these reasons, processing in this way is only permitted by the UK GDPR in limited circumstances. These include where to provide the privacy information proves **impossible** or would involve a **disproportionate effort**.

Circumstances when it is impossible to provide privacy will only arise rarely, for example where you have no contact details for individuals and have no reasonable means of obtaining them.

It is important that you can demonstrate compliance with individuals' right to be informed. So, if you are proposing processing operations that involve the use of data obtained from third parties, you must first carefully consider whether you can provide privacy information to the individuals. If you intend to rely on the exception for disproportionate effort, you must be able to justify this, and you must take other measures to protect people's rights. In particular, you must still publish your privacy information, and carry out a DPIA.

Your DPIA will help you assess and demonstrate whether you are taking a proportionate approach. It will help you consider how best to mitigate the impact on individuals' ability to exercise control over their data, and whether you can take other measures to support the exercise of their rights. It will also help you demonstrate how you comply with fairness and transparency requirements.

In more detail – ICO guidance

Read the ICO guidance on the right to be informed, which includes a section on disproportionate effort and other exceptions and exemptions.

Further reading – European Data Protection Board

See the WP29 guidelines on Transparency, which have been endorsed by the EDPB.

Further Reading

Relevant provisions in the UK GDPR - See Articles 14(1), (2) and (5) and Recitals 60, 61 and 62
External link

What does 'vulnerable individual' mean?

Individuals can be vulnerable where circumstances may restrict their ability to freely consent or object to the processing of their personal data, or to understand its implications.

Most obviously, children are regarded as vulnerable to the processing of their personal data since they may be less able to understand how their data is being used, anticipate how this might affect them, and protect themselves against any unwanted consequences. This can also be true of other vulnerable sections of the population such as elderly people, or those with certain disabilities.

Even if the individuals are not part of a group you might automatically consider vulnerable, an imbalance of power in their relationship with you can cause vulnerability for data protection purposes if they believe that they will be disadvantaged if the processing doesn't go ahead.

One group who may count as vulnerable in this sense are employees. The European guidelines on DPIAs (WP248) explain why employees could be considered vulnerable data subjects where a power imbalance means they cannot easily consent or object to the processing of their data by an employer. This type of vulnerability could also arise due to an individual's financial situation (e.g. credit rating) or the specific context of the processing (e.g. patients receiving medical care).

Processing the data of individuals who may be deemed vulnerable is one of the criteria in European guidelines for processing likely to result in high risk. If you think your processing will involve vulnerable individuals, then a DPIA will be required should any of the other criteria, or operations on our list, be engaged.

Example

A sales firm provides company cars for their employees, and intends to deploy vehicles with location-tracking features, allowing managers to monitor the movement and whereabouts of their employees at

all times. Employees are also permitted to use the vehicles for their private purposes outside working hours.

The processing intends to track each individual's geolocation, in a context where they are vulnerable to a power imbalance with the controller. So this engages the requirement for a DPIA to identify and mitigate the risks to the employees' rights and freedoms.

Further Reading

Relevant provisions in the UK GDPR - See Articles 35(3) and Recitals 38, 75 and 91
External link

In more detail – ICO guidance

Read our guidance on children and the UK GDPR for more on consent and the extra protections for children.

Further reading – European Data Protection Board

WP29 produced guidelines on data protection impact assessments, which have been endorsed by the EDPB.

Read the WP29 Opinion 2/2017 on data processing at work for more on the processing of personal data in an employment context.

What does 'large scale' mean?

Again, the UK 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.

Further Reading

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

Further reading – European Data Protection Board

WP29 produced guidelines on data protection impact assessments, which have been endorsed by the EDPB.

Also read the WP29 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 are not subject to other obligations to complete DPIAs derived from specific legislation, such as Digital Economy Act 2017;
  - 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; and
  - 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. So in the absence of any clear and authoritative statement on whether such an assessment was done, we recommend you err on the side of caution and do 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.

Further Reading

Relevant provisions in the UK GDPR - See Articles 35(4) and (10)
External link

Further reading – European Data Protection Board

WP29 produced guidelines on data protection impact assessments, which have been endorsed by the EDPB.

How do we do a DPIA?

In detail

- What are the key elements of a DPIA process?
- Is there a template we can use?
- Who should do the DPIA?
- What is the role of the DPO?
- Step 1: How do we decide whether to do a DPIA?
- Step 2: How do we describe the processing?
- Step 3: Do we need to consult individuals?
- Step 3: Do we need to consult anyone else?
- Step 4: How do we assess necessity and proportionality?
- Step 5: How do we identify and assess risks?
- Step 6: How do we identifying mitigating measures?
- Step 7: How do we conclude our DPIA?
- What happens next?

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

After sign-off you should integrate the outcomes from your DPIA back into your project plan, and keep your DPIA under review. Throughout this process, you should consult individuals and other stakeholders as needed.

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.

Further Reading

Relevant provisions in the UK GDPR - See Articles 35(2), (7) and (9)
External link

Further reading

WP29 produced guidelines on data protection impact assessments, which have been endorsed by the EDPB. Annex 2 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 make your own to suit your needs, or use an existing project-management method, as long as it covers all the key elements of the process. If you are making your own template, you may 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 in your organisation, and who signs them off. You can outsource your DPIA, but you remain responsible for it. If you have a Data Protection Officer (DPO), you must ask for their advice on your DPIA, and document it as part of the process.

You may want to ask a processor to carry out a DPIA on your behalf if they do the relevant processing operation, but again you remain responsible for it.

Who should be involved in the DPIA?

As well as the business area or individual who is leading on the project or process requiring the DPIA, you should also involve:

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

Further reading

WP29 produced guidelines on data protection impact assessments, which have been endorsed by the EDPB.

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 DPIA's ongoing performance, including how well you have implemented your planned actions to address the risks.

Under Article 39 of UK GDPR, DPOs have specific tasks regarding DPIAs. This is why you must ensure that any responsibilities you give a DPO for your DPIA do not conflict with their ability to complete these tasks in an independent manner, as required by Recital 97.

Further Reading

Relevant provisions in the UK GDPR - See Articles 35(2)and 39(1)(c)
External link

In more detail – ICO guidance

Read our guidance on data protection officers for more detail on the tasks for DPOs regarding DPIAs.

Further reading – European Data Protection Board

Read the WP29 Guidelines on Data Protection Officers (WP243).

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

Ask your DPO for advice. If you have any major project that involves the use of personal data, it is good practice to do 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 that automatically require a DPIA. If not, you need to screen for other factors that may indicate it is a type of processing that is likely to result in high risk, such as processing the data of vulnerable individuals.

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

If you do this screening and decide a DPIA is not needed, you should document your decision and the reasons for it, including your DPO's advice. This does not have to be a burdensome paperwork exercise. It just needs to help you demonstrate 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;

- how far individuals have control over their data;
- how far individuals are likely to expect the processing;
- whether these individuals 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;
- in due course, whether you comply with any UK GDPR codes of conduct (once any have been approved under Article 40) or UK GDPR certification schemes;and
- 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.

Further Reading

> Relevant provisions in the UK GDPR - See Article 35(7)(a) and Recitals 84, 90 and 94
> External link

Step 3: Do we need to consult individuals?

You should seek and document 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 this is not appropriate, you should record this decision as part of your DPIA, with a clear explanation. For example, you may 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 market research with a certain demographic or contacting relevant campaign or consumer groups for their views.

If your DPIA decision differs from the views of individuals, you need to document your reasons for disregarding their views.

Further Reading

Relevant provisions in the https://www.legislation.gov.uk/eur/2016/679/contentsGDPR - See Article 35(9)
External link

Further reading

WP29 produced guidelines on data protection impact assessments, which have been endorsed by the EDPB.

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.

Further Reading

Relevant provisions in the UK GDPR - See Article 28(3)(f)
External link

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?

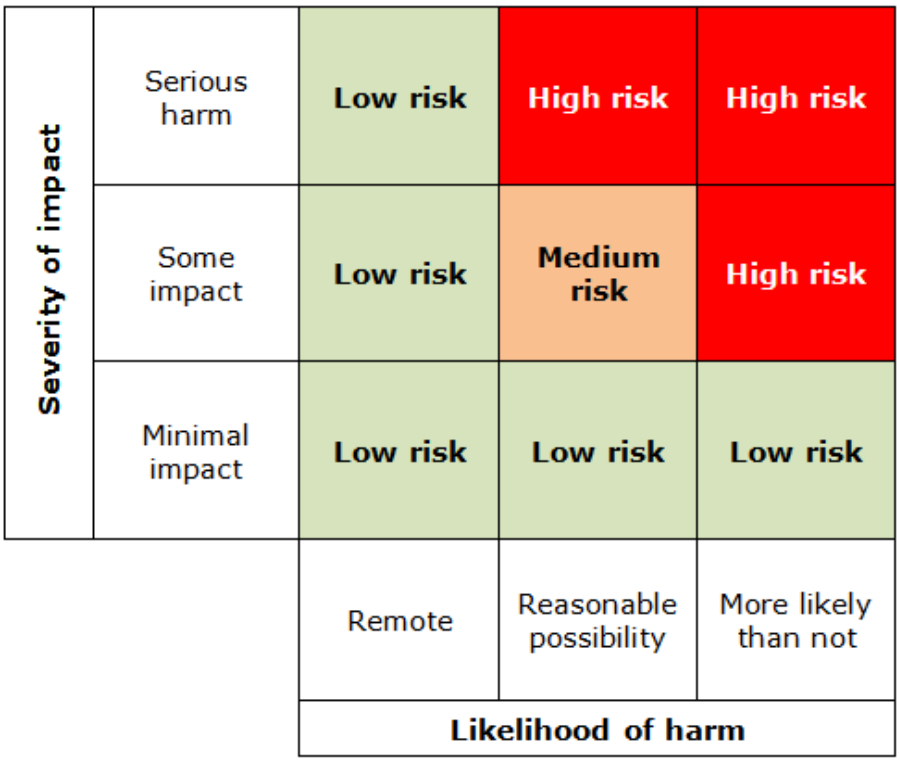
Consider the potential impact on individuals and any harm or damage your processing may cause – whether physical, emotional or material. In particular, look at whether the processing could contribute to:

- 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;
- re-identification 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 to 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 may still count as high risk.

You must make an objective assessment of the risks. It is helpful to use a structured matrix to think about likelihood and severity of risks:



The above matrix shows a structured way to assess risk. Your organisation may use a different method you can adapt for the same purpose.

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

Further Reading

Relevant provisions in the UK GDPR - See Articles 35(7)(c) and Recitals 76 and 90
External link

Step 6: How do we identify mitigating measures?

Against each risk identified, record its source. 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;
- 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 seek and document DPO advice 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 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 must consult the ICO before you go ahead with the processing. See the next section for more information on this consultation process.

To aid transparency and accountability, it is good practice to publish your DPIA. This could help foster trust in your processing activities, and improve individuals' ability to exercise their rights. If you are concerned that publication may 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.

When considering publishing DPIAs, public authorities should think about their wider transparency

obligations, such as complying with the Freedom of Information Act. Before UK GDPR, many public authorities included privacy impact assessments in their definition documents for publication schemes.

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

Further Reading

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

Further reading

WP29 produced guidelines on data protection impact assessments, which have been endorsed by the EDPB.

Do we need to consult the ICO?

In detail

- When do we need to consult the ICO?
- How do we consult the ICO?
- What happens next?
- What happens if we do not accept your DPIA?
- How is our DPIA assessed?
- How long does it take?
- What are the possible outcomes?
- Can we appeal?

When do we need to consult the ICO?

If you have carried out a DPIA that identifies a high risk and you cannot do anything to reduce it, prior consultation with the ICO is required under UK GDPR. You cannot go ahead with the processing until you have consulted us.

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

Further Reading

> Relevant provisions in the UK GPDR - See Article 36(1) and Recital 94
> External link

Further reading - European Data Protection Board

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?

Send us a copy of your submission. 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 (if you have one); and

- a copy of the DPIA.

Further Reading

> Key provisions in the UK GDPR - See Article 36(3)
> External link

What happens next?

When we receive your DPIA, we will send you an acknowledgement and check we have all the information we need.

We will write to you to within 10 days to let you know if we have accepted your DPIA for prior consultation. We will explain our reasoning.

You may not hear from us again until we provide our written advice. If we have further queries, we may make contact to arrange a telephone call or meeting with you.

Further Reading

> Relevant provisions in the UK GDPR - See Article 36(2)
> External link

What happens if we do not accept your DPIA?

We may wish to discuss your proposed processing with you, even if your DPIA does not meet the criteria for prior consultation. If so, we will explain to you how we would like to engage with you.

How is your DPIA assessed?

If we accept your DPIA, we don't just look at the risks you documented. We consider all of your submission – your DPIA documentation and any further information you provided – along with any prior contact you may have had with our office.

We seek to understand in detail the context and nature of the processing you are proposing, including any controller-processor relationships. We will also assess the extent to which you have evidenced compliance with the Data Protection Principles.

To do this effectively, we may need to ask you to give us more information.

How long does it take?

Where we provide advice under the prior consultation process, we will get back to you within eight weeks of receipt of your DPIA. In complex cases, we can 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. We will explain our reasons.

If we need to ask for more information, we cannot continue our assessment until you provide it. To prevent further delay, please ensure you include any documents your assessment refers to, such as privacy notices.

If your intended processing operation would affect data subjects in EU member states, we may be required to co-operate with other data protection authorities before providing our written advice, in line with Chapter VII UK GDPR. This may mean your case cannot be resolved in 14 weeks. We will notify you if this occurs and keep you updated.

Further Reading

> Relevant provisions in the UK GDPR - See Article 36(2)
> External link

What are the possible outcomes?

We may come to the view, based on your DPIA, that risks have been sufficiently identified and mitigated, and that you may proceed with the processing.

Our written response could be limited to advice on how you can further mitigate identified risks before you proceed with your processing.

In some circumstances, we may also issue an official warning, a new corrective power under UK GDPR, alongside any advice we provide. We will issue warnings where we are concerned that your intended processing is likely to contravene UK GDPR. Any warning will explain the reasons for our concerns, and the steps we recommend you take to avoid any contravention.

If we have more significant concerns, we may impose a limitation or ban on your intended processing.

In any outcome, our written response to you will make clear what you may and may not do.

Further Reading

> Key provisions in the UK GDPR - See Articles 36(2) and 58
> External link

Can we appeal?

Warnings are not subject to appeal, but you may seek judicial review if you disagree with the way we made the decision.

You can seek a review of other corrective measures (such as limitations or bans on processing) by appeal to the First Tier Tribunal.

More information on appeals against the Information Commissioner can be found here.

Examples of processing 'likely to result in high risk'

The following list details processing operations for which the ICO requires you to complete a DPIA as they are 'likely to result in high risk'. It is based on guidelines adopted by the European Data Protection Board (EDPB) on DPIAs (WP248rev01). Our list therefore complements and further specifies these guidelines.

For illustration, we have also included examples of existing areas of application. These should not be taken as definitive or exhaustive. In any event, this list does not affect your overriding obligation in Article 35(1), which is to assess any proposed processing operation against the requirement to complete DPIAs. The ICO also considers it best practice to do a DPIA, whether or not the processing is likely to result in a high risk.

Type of processing operation(s) requiring a DPIA	Description	Non-exhaustive examples of existing areas of application
Innovative technology	Processing involving the use of new technologies, or the novel application of existing technologies (including AI). A DPIA is required for any intended processing operation(s) involving innovative use of technologies (or applying new technological and/or organisational solutions) when combined with any other criterion from WP248rev01.	• Artificial intelligence, machine learning and deep learning • Connected and autonomous vehicles • Intelligent transport systems • Smart technologies (including wearables) • Market research involving neuro-measurement (i.e. emotional response analysis and brain activity) • Some IoT applications, depending on the specific circumstances of the processing
Denial of service	Decisions about an individual's access to a product, service, opportunity or benefit which are based to any extent on automated decision-making (including profiling) or involves the processing of special-category data.	• Credit checks • Mortgage or insurance applications • Other pre-check processes related to contracts (i.e. smartphones)
Large-scale profiling	Any profiling of individuals on a large scale	• Data processed by Smart Meters or IoT applications • Hardware/software offering fitness/lifestyle monitoring • Social-media networks • Application of AI to existing

		process
Biometric data	Any processing of biometric data for the purpose of uniquely identifying an individual. A DPIA is required for any intended processing operation(s) involving biometric data for the purpose of uniquely identifying an individual, when combined with any other criterion from WP248rev01	• Facial recognition systems • Workplace access systems/identity verification • Access control/identity verification for hardware/applications (including voice recognition/fingerprint/facial recognition)
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 for any intended processing operation(s) involving genetic data when combined with any other criterion from WP248rev01	• Medical diagnosis • DNA testing • Medical research
Data matching	Combining, comparing or matching personal data obtained from multiple sources	• Fraud prevention • Direct marketing • Monitoring personal use/uptake of statutory services or benefits • Federated identity assurance services
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 (as provided by Article 14.5(b). A DPIA is required for any intended processing operation(s) involving where the controller is relying on	• List brokering • Direct marketing • Online tracking by third parties • Online advertising • Data aggregation/data aggregation platforms • Re-use of publicly available data

	Article 14.5(b) when combined with any other criterion from WP248rev01	
Tracking	Processing which involves tracking an individual's geolocation or behaviour, including but not limited to the online environment. A DPIA is required for any intended processing operation involving geolocation data when combined with any other criterion from WP248rev01	• Social networks, software applications • Hardware/software offering fitness/lifestyle/health monitoring • IoT devices, applications and platforms • Online advertising • Web and cross-device tracking • Data aggregation / data aggregation platforms • Eye tracking • Data processing at the workplace • Data processing in the context of home and remote working • Processing location data of employees • Loyalty schemes • Tracing services (tele-matching, tele-appending) • Wealth profiling – identification of high net-worth individuals for the purposes of direct marketing
Targeting of children/other vulnerable individuals for marketing, profiling for auto decision making or the offer of online services	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.	• Connected toys • Social networks
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.	• Whistleblowing/complaint procedures • Social care records