Data protection by design and default

At a glance

- The GDPR requires you to put in place appropriate technical and organisational measures to implement the data protection principles and safeguard individual rights. This is 'data protection by design and by default'.
- In essence, this means you have to integrate or 'bake in' data protection into your processing activities and business practices, from the design stage right through the lifecycle.
- This concept is not new. Previously known as 'privacy by design', it has have always been part of data protection law. The key change with the GDPR is that it is now a legal requirement.
- Data protection by design is about considering data protection and privacy issues upfront in everything you do. It can help you ensure that you comply with the GDPR's fundamental principles and requirements, and forms part of the focus on accountability.

Checklists

☐ We consider data protection issues as part of the design and implementation of systems, services, products and business practices.

☐ We make data protection an essential component of the core functionality of our processing systems and services.

☐ We anticipate risks and privacy-invasive events before they occur, and take steps to prevent harm to individuals.

☐ We only process the personal data that we need for our purposes(s), and that we only use the data for those purposes.

☐ We ensure that personal data is automatically protected in any IT system, service, product, and/or business practice, so that individuals should not have to take any specific action to protect their privacy.

☐ We provide the identity and contact information of those responsible for data protection both within our organisation and to individuals.

☐ We adopt a 'plain language' policy for any public documents so that individuals easily understand what we are doing with their personal data.

☐ We provide individuals with tools so they can determine how we are using their personal data, and whether our policies are being properly enforced.

☐ We offer strong privacy defaults, user-friendly options and controls, and respect user preferences.

☐ We only use data processors that provide sufficient guarantees of their technical and organisational measures for data protection by design.

☐ When we use other systems, services or products in our processing activities, we make sure that we only use those whose designers and manufacturers take data protection issues into account.

☐ We use privacy-enhancing technologies (PETs) to assist us in complying with our data protection by design obligations.

In brief

What's new in the GDPR?

The GDPR introduces new obligations that require you to integrate data protection concerns into every aspect of your processing activities. This approach is 'data protection by design and by default'. These are key elements of the GDPR's risk-based approach and its focus on accountability, ie you are able to demonstrate how you are complying with its requirements.

However, data protection by design and by default is not new. It is essentially the GDPR's version of 'privacy by design', an approach that the ICO has championed for many years. Although privacy by design and data protection by design are not precisely the same, there are well-established privacy by design principles and practices that can apply in this context.

Some organisations already adopt a 'privacy by design approach' as a matter of good practice. If this is the case for you, then you are well-placed to meet the requirements of data protection by design and by default. Although you may still need to review your processes and procedures to ensure that you are meeting your obligations.

The biggest change is that whilst privacy by design was good practice under the Data Protection Act 1998 (the 1998 Act), data protection by design and by default are legal requirements under the GDPR.

What does the GDPR say about data protection by design and by default?

Articles 25(1) and 25(2) of the GDPR outline your obligations concerning data protection by design and by default.

Article 25(1) specifies the requirements for data protection by design:

> ‘Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, 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, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.’

Article 25(2) specifies the requirements for data protection by default:

> ‘The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.’

Article 25(3) states that if you adhere to an approved certification under Article 42, you can use this as one way of demonstrating your compliance with these requirements.

Further Reading

> Relevant provisions in the GDPR - Article 25 and Recital 78
> External link

What is data protection by design?

Data protection by design is ultimately an approach that ensures you consider privacy and data protection issues at the design phase of any system, service, product or process and then throughout the lifecycle.

As expressed by the GDPR, it requires you to:

- put in place appropriate technical and organisational measures designed to implement the data

protection principles; and

- integrate safeguards into your processing so that you meet the GDPR's requirements and protect the individual rights.

In essence this means you have to integrate or 'bake in' data protection into your processing activities and business practices.

Data protection by design has broad application. Examples include:

- developing new IT systems, services, products and processes that involve processing personal data;
- developing organisational policies, processes, business practices and/or strategies that have privacy implications;
- physical design;
- embarking on data sharing initiatives; or
- using personal data for new purposes.

The underlying concepts of data protection by design are not new. Under the name 'privacy by design' they have existed for many years. Data protection by design essentially inserts the privacy by design approach into data protection law.

Under the 1998 Act, the ICO supported this approach as it helped you to comply with your data protection obligations. It is now a legal requirement.

What is data protection by default?

Data protection by default requires you to ensure that you only process the data that is necessary to achieve your specific purpose. It links to the fundamental data protection principles of data minimisation and purpose limitation.

You have to process some personal data to achieve your purpose(s). Data protection by default means you need to specify this data before the processing starts, appropriately inform individuals and only process the data you need for your purpose. It does **not** require you to adopt a 'default to off' solution. What you need to do depends on the circumstances of your processing and the risks posed to individuals.

Nevertheless, you must consider things like:

- adopting a 'privacy-first' approach with any default settings of systems and applications;
- ensuring you do not provide an illusory choice to individuals relating to the data you will process;
- not processing additional data unless the individual decides you can;
- ensuring that personal data is not automatically made publicly available to others unless the individual decides to make it so; and
- providing individuals with sufficient controls and options to exercise their rights.

Who is responsible for complying with data protection by design and by default?

Article 25 specifies that, as the controller, you have responsibility for complying with data protection by design and by default. Depending on your circumstances, you may have different requirements for different areas within your organisation. For example:

- your senior management, eg developing a culture of 'privacy awareness' and ensuring you develop policies and procedures with data protection in mind;
- your software engineers, system architects and application developers, –eg those who design systems, products and services should take account of data protection requirements and assist you in complying with your obligations; and
- your business practices, eg you should ensure that you embed data protection by design in all your internal processes and procedures.

This may not apply to all organisations, of course. However, data protection by design is about adopting an organisation-wide approach to data protection, and 'baking in' privacy considerations into any processing activity you undertake. It doesn't apply only if you are the type of organisation that has your own software developers and systems architects.

In considering whether to impose a penalty, the ICO will take into account the technical and organisational measures you have put in place in respect of data protection by design. Additionally, under the Data Protection Act 2018 (DPA 2018) we can issue an Enforcement Notice against you for any failings in respect of Article 25.

What about data processors?

If you use another organisation to process personal data on your behalf, then that organisation is a data processor under the GDPR.

Article 25 does not mention data processors specifically. However, Article 28 specifies the considerations you must take whenever you are selecting a processor. For example, you must only use processors that provide:

> "
>
> 'sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject'

This requirement covers both data protection by design in Article 25 as well as your security obligations under Article 32. Your processor cannot necessarily assist you with your data protection by design obligations (unlike with security measures), however you must only use processors that provide sufficient guarantees to meet the GDPR's requirements.

What about other parties?

Data protection by design and by default can also impact organisations other than controllers and processors. Depending on your processing activity, other parties may be involved, even if this is just where you purchase a product or service that you then use in your processing. Examples include manufacturers, product developers, application developers and service providers.

Recital 78 extends the concepts of data protection by design to other organisations, although it does not place a requirement on them to comply – that remains with you as the controller. It says:

> ‘When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations.’

Therefore, when considering what products and services you need for your processing, you should look to choose those where the designers and developers have taken data protection into account. This can help to ensure that your processing adheres to the data protection by design requirements.

If you are a developer or designer of products, services and applications, the GDPR places no specific obligations on you about how you design and build these products. (You may have specific obligations as a controller in your own right, eg for any employee data.) However, you should note that controllers are required to consider data protection by design when selecting services and products for use in their data processing activities – therefore if you design these products with data protection in mind, you may be in a better position.

Further Reading

Relevant provisions in the GDPR - Articles 25 and 28, and Recitals 78, 79, 81 and 82
External link

What are we required to do?

You must put in place appropriate technical and organisational measures designed to implement the data protection principles and safeguard individual rights.

There is no ‘one size fits all’ method to do this, and no one set of measures that you should put in place. It depends on your circumstances.

The key is that you consider data protection issues from the start of any processing activity, and adopt appropriate policies and measures that meet the requirements of data protection by design and by default.

Some examples of how you can do this include:

- minimising the processing of personal data;
- pseudonymising personal data as soon as possible;
- ensuring transparency in respect of the functions and processing of personal data;
- enabling individuals to monitor the processing; and
- creating (and improving) security features.

This is not an exhaustive list. Complying with data protection by design and by default may require you to do much more than the above.

However, we cannot provide a complete guide to all aspects of data protection by design and by default in all circumstances. This guidance identifies the main points for you to consider. Depending on the processing you are doing, you may need to obtain specialist advice that goes beyond the scope of this guidance.

Further Reading

> Relevant provisions in the GDPR - Recital 78
> External link

When should we do this?

You should begin data protection by design at the initial phase of any system, service, product, or process. You should start by considering your intended processing activities, the risks that these may pose to individuals, and the possible measures available to ensure that you comply with the data protection principles and protect individual rights. These considerations must cover:

- the state of the art and costs of implementation of any measures;
- the nature, scope, context and purposes of your processing; and
- the risks that your processing poses to the rights and freedoms of individuals.

This is similar to the information risk assessment you should do when considering your security measures.

These considerations lead into the second step, where you put in place actual technical and organisational measures to implement the data protection principles and integrate safeguards into your processing.

This is why there is no single solution or process that applies to every organisation or every processing activity, although there are a number of commonalities that may apply to your specific circumstances as described below.

The GDPR requires you to take these actions:

- 'at the time of the determination of the means of the processing' – in other words, when you are at the design phase of any processing activity; and
- 'at the time of the processing itself' – ie during the lifecycle of your processing activity.

What are the underlying concepts of data protection by design and by default?

The underlying concepts are essentially expressed in the seven 'foundational principles' of privacy by design, as developed by the Information and Privacy Commissioner of Ontario.

Although privacy by design is not necessarily equivalent to data protection by design, these foundational principles can nevertheless underpin any approach you take.

'Proactive not reactive; preventative not remedial'

You should take a proactive approach to data protection and anticipate privacy issues and risks before they happen, instead of waiting until after the fact. This doesn't just apply in the context of systems

design – it involves developing a culture of 'privacy awareness' across your organisation.

'Privacy as the default setting'

You should design any system, service, product, and/or business practice to protect personal data automatically. With privacy built into the system, the individual does not have to take any steps to protect their data – their privacy remains intact without them having to do anything.

'Privacy embedded into design'

Embed data protection into the design of any systems, services, products and business practices. You should ensure data protection forms part of the core functions of any system or service – essentially, it becomes integral to these systems and services.

'Full functionality – positive sum, not zero sum'

Also referred to as 'win-win', this principle is essentially about avoiding trade-offs, such the belief that in any system or service it is only possible to have privacy **or** security, not privacy **and** security. Instead, you should look to incorporate all legitimate objectives whilst ensuring you comply with your obligations.

'End-to-end security – full lifecycle protection'

Put in place strong security measures from the beginning, and extend this security throughout the 'data lifecycle' – ie process the data securely and then destroy it securely when you no longer need it.

'Visibility and transparency – keep it open'

Ensure that whatever business practice or technology you use operates according to its premises and objectives, and is independently verifiable. It is also about ensuring visibility and transparency to individuals, such as making sure they know what data you process and for what purpose(s) you process it.

'Respect for user privacy – keep it user-centric'

Keep the interest of individuals paramount in the design and implementation of any system or service, eg by offering strong privacy defaults, providing individuals with controls, and ensuring appropriate notice is given.

How do we do this in practice?

One means of putting these concepts into practice is to develop a set of practical, actionable guidelines that you can use in your organisation, framed by your assessment of the risks posed and the measures available to you. You could base these upon the seven foundational principles.

However, how you go about doing this depends on your circumstances – who you are, what you are doing, the resources you have available, and the nature of the data you process. You may not need to have a set of documents and organisational controls in place, although in some situations you will be required to have certain documents available concerning your processing.

The key is to take an organisational approach that achieves certain outcomes, such as ensuring that:

- you consider data protection issues as part of the design and implementation of systems, services,

products and business practices;

- you make data protection an essential component of the core functionality of your processing systems and services;
- you only process the personal data that you need in relation to your purposes(s), and that you only use the data for those purposes;
- personal data is automatically protected in any IT system, service, product, and/or business practice, so that individuals should not have to take any specific action to protect their privacy;
- the identity and contact information of those responsible for data protection are available both within your organisation and to individuals;
- you adopt a 'plain language' policy for any public documents so that individuals easily understand what you are doing with their personal data;
- you provide individuals with tools so they can determine how you are using their personal data, and whether you are properly enforcing your policies; and
- you offer offering strong privacy defaults, user-friendly options and controls, and respect user preferences.

Many of these relate to other obligations in the GDPR, such as transparency requirements, documentation, Data Protection Officers and DPIAs. This shows the broad nature of data protection by design and how it applies to all aspects of your processing. Our guidance on these topics will help you when you consider the measures you need to put in place for data protection by design and by default.

In more detail – ICO guidance

Read our sections on the data protection principles, individual rights, accountability and governance, documentation, data protection impact assessments, data protection officers and security in the Guide to the GDPR.

In more detail – European Data Protection Board

The European Data Protection Board (EDPB), which has replaced the Article 29 Working Party (WP29), includes representatives from the data protection authorities of each EU member state. It adopts guidelines for complying with the requirements of the GDPR.

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

Further reading

We will produce further guidance on how you can implement data protection by design soon. However, the Information and Privacy Commissioner of Ontario has published guidance on how organisations can 'operationalise' privacy by design, which may assist you.

How do data protection by design and by default link to data protection impact assessments (DPIAs)?

A DPIA is a tool that you can use to identify and reduce the data protection risks of your processing activities. They can also help you to design more efficient and effective processes for handling personal data.

DPIAs are an integral part of data protection by design and by default. For example, they can determine the type of technical and organisational measures you need in order to ensure your processing complies with the data protection principles.

However, a DPIA is only required in certain circumstances, such as where the processing is likely to result in a risk to rights and freedoms, though it is good practice to undertake a DPIA anyway. In contrast, data protection by design is a broader concept, as it applies organisationally and requires you to take certain considerations even before you decide whether your processing is likely to result in a high risk or not.

In more detail – ICO guidance

Read our guidance on DPIAs in the Guide to the GDPR.

We have also produced more detailed guidance on DPIAs, including a template that you can use and a list of processing operations that we consider require DPIAs to be undertaken.

In more detail – European Data Protection Board

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

What is the role of privacy-enhancing technologies (PETs)?

Privacy-enhancing technologies or PETs are technologies that embody fundamental data protection principles by minimising personal data use, maximising data security, and empowering individuals. A useful definition from the European Union Agency for Network and Information Security (ENISA) refers to PETs as:

> ‘software and hardware solutions, ie systems encompassing technical processes, methods or knowledge to achieve specific privacy or data protection functionality or to protect against risks of privacy of an individual or a group of natural persons.’

PETs link closely to the concept of privacy by design, and therefore apply to the technical measures you can put in place. They can assist you in complying with the data protection principles and are a means of implementing data protection by design within your organisation on a technical level.

Further reading

We will provide further guidance on PETs in the near future. ENISA has also published research reports on PETs that may assist you.

What about international transfers?

Data protection by design also applies in the context of international transfers in cases where you intend to transfer personal data overseas to a third country that does not have an adequacy decision.

You need to ensure that, whatever mechanism you use, appropriate safeguards are in place for these transfers. As detailed in Recital 108, these safeguards need to include compliance with data protection by design and by default.

Further Reading

Relevant provisions in the GDPR - Article 47 and Recital 108
External link

In more detail – ICO guidance

Read our guidance on international transfers.

What is the role of certification?

Article 25(3) says that:

> ‘An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article.’

This means that an approved certification mechanism, once one is available, can assist you in showing how you are complying with, and implementing, data protection by design and by default.

In more detail – European Data Protection Board

The EDPB published for consultation draft guidelines on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679 on 30 May 2018. The consultation closed on 12 July 2018.

What additional guidance is available?

The ICO will publish more detailed guidance about data protection by design and privacy enhancing technologies soon, as well as how these concepts apply in the context of the code of practice on age appropriate design in the DPA 2018 section 123.

In the meantime, there are a number of publications about the privacy by design approach. We have summarised some of these below.

Further reading

The **Information and Privacy Commissioner of Ontario** (IPC) originated the concept of privacy by design in the 1990s. The IPC has a number of relevant publications about the concept and how you can implement it in your organisation, including:

- the original seven foundational principles of privacy by design (external link, PDF); and
- a primer on privacy by design, published in 2013 (external link, PDF); and
- guidance on Operationalizing privacy by design, published in 2012 (external link, PDF)

The **European Union Agency for Network and Information Security** (ENISA) has also published research and guidance on privacy by design, including:

- a research report on privacy and data protection by design (external link);
- a research report on privacy by design and big data (external link); and
- a subsection on privacy-enhancing technologies (external link)

The **Norwegian data protection authority** (Datatilsynet) has produced guidance on how software developers can implement data protection by design and by default.

Data protection impact assessments

Click here for information about consulting the ICO about your data protection impact assessment.

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?

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 email us and attach 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 – European Data Protection Board

The European Data Protection Board (EDPB), which has replaced the Article 29 Working Party (WP29), includes representatives from the data protection authorities of each EU member state. It adopts guidelines for complying with the requirements of the GDPR.

WP29 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), which have been endorsed by the EDPB.

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)