GDPR - Data Protection Impact Assessment (DPIA)

Do any organisational changes involve GDPR ....?

INTRODUCTION TO THE DPIA ARRANGE FREE GDPR CONSULTATION (INDEX.HTML#FREE)

Arrange A FREE GDPR Consultation (Index.Html#FREE)

(index.html#FREE)

Introduction to Data Protection Impact Assessment

What is a Data Protection Impact Assessment?

Whenever you undertake any change within your organisation as a project there will need to be a process designed to help you systematically analyse, identify and minimise the data protection risks of this 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.

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.

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.

Click here (GDPR_Conduct_DPIA.html) for instructions on how to perform a DPIA.