Firebird
Data Protection Consultancy Ltd

Data Protection Impact Assessments: Short Guide

What is a DPIA?

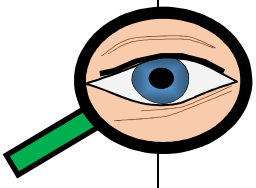
A DPIA (otherwise known as a Data Protection Impact Assessment) is when you identify, analyse and minimise the data protection risks around certain activities involving people's data.

When do we need one?

The data protection legislation requires organisations to carry out a DPIA if they are going to process personal data (e.g. collect, use, store, share or delete personal data), which could have a negative impact on people's rights and freedoms. It is particularly important to carry out a DPIA when you want to use new technology, as this could increase the likelihood of a data protection breach occurring and the impact on the people involved.

You will need to carry out a DPIA in cases where your proposed activity is 'high risk' and could result in the following **impact** to individuals:

- they could suffer discrimination; identity theft or fraud; financial loss; reputational damage; physical harm or loss of confidentiality **if a breach occurred;**
- it will stop them from exercising their privacy or other legal rights;
- it will inhibit their ability to access services or opportunities;
- they could lose control over the use of their data;
- they will suffer significant economic or social disadvantage.



What activities could be 'high risk'?

There are several 'high risk' activities which organisations carry out which are likely to require a DPIA. For example:

- Installing or upgrading **CCTV**.
- Purchasing a new system that will store personal data in the **Cloud.**
- Installing a visitor management system that will collect **photographs** and other personal data.
- Putting in place a system that will store lots of highly personal or **sensitive** data.
- Setting up employee **remote access** to the organisation's customer management system and other systems.
- Implementing innovative technology which uses personal data e.g. technology which **monitors or tracks** employees.
- Collecting **fingerprints** or retina scans to enable access to systems or restricted areas.
- Using **radios** for employees to communicate with each other.
- **Publishing photographs** and videos of vulnerable people who are identifiable.
- Setting up **automated** file deletion rules in email and other systems.
- **Monitoring** employees' or visitors' email or internet activity.
- **Transferring** large amounts of personal data from one system to another.

Firebird
Data Protection Consultancy Ltd

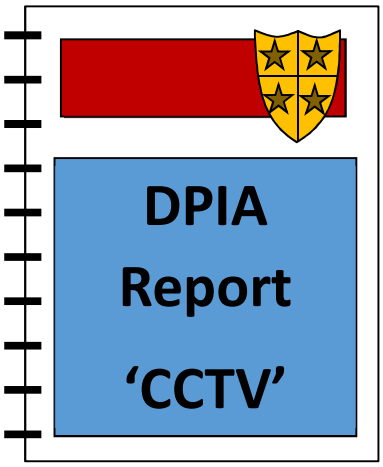
What should our DPIAs cover?

When carrying out your assessment, you should identify, assess and document the following information:

- A **description** of the personal data you want to process and the reason why.
- A description of the **measurers** you will put in place to comply with the data protection principles.
- A description of the **potential risks** to individuals and an assessment of the **impact** of those risks.
- A description of the actions that will be taken to **reduce the likelihood** of the risks occurring.
- The **remaining risk level** after the actions will be put in place.
- Comments and **recommendations** made by your Data Protection Officer (DPO).
- **Decision** from senior management whether to go ahead with the proposed activity.
- Date when the DPIA should be **reviewed** by the DPO (e.g. annually or if any of the risks or actions change).

DPIAs should be carried out by someone with **knowledge of the proposed activity** and the **potential impact** it may have. Ideally, this should be a member of the Senior Management Team (SMT) in consultation with the IT lead where relevant.

The **DPO should remain independent**; their role is to advise when a DPIA is required and whether the activity will comply with the data protection laws. The final decision to go ahead rests with the SLT member, after careful consideration of the DPO's advice.



What are the potential risks?

There could be many different data protection risks associated with activities, which you need to look out for. This will depend on what you intend to do with the data, but here are some examples of risk types:

- **Unauthorised access** to confidential or sensitive data.
- Vital information cannot be accessed quickly due to **IT failures**.
- **Unauthorised sharing** or use of personal data.
- Data is accidentally **lost or destroyed**.
- **Inaccurate data** could be used or shared.
- System could be vulnerable to hacking or **malicious activities**.
- **Covert monitoring** could take place.
- Communications may be **intercepted** by unauthorised persons.
- Data is collected, used or shared without an appropriate **legal basis**.
- Individuals are **not aware** of how their data is being processed.
- **Excessive information** may be collected.
- Data **cannot be deleted** from the system in line with retention schedules.

You should also include any business **risks** too.

How can we reduce the likelihood of the risks occurring?

There are many ways in which you can do this, here are some examples:

- Ensure everyone who handles personal data receives **appropriate training**, so they know how to access, use, share, store or destroy the data properly and in line with your organisation's policy.
- **Restrict access** to paper and electronic information only to the individuals who need access to it.
- Update your **privacy notices** to explain any new uses or sharing.
- Ensure there are robust **IT security** measures in place to defend against intruders, unauthorised modifications to the data and malicious software on your network.
- Identify the **legal basis** for processing the data with your Data Protection Officer.
- Use a system that enables data to be **deleted** or amended when required.
- Reduce the amount of data being processed or **don't use identifiable** personal data if it's not strictly needed.
- **Encrypt** portable equipment that contains personal data such as laptops and removable media.
- Carry out annual or more regular **checks** to ensure data is accurate and up to date.

How do we decide if it's ok to go ahead?

As part of your assessment, you should evaluate and document what your risks and impacts are; the level of impact on the data subjects and the likelihood of the risks occurring; what actions you intend to take to reduce them and the final risk level after the actions have been applied.

You may wish to record this information in a table like this:

Risks & impact	Level of impact & likelihood of risk	Actions to reduce or eliminate Risk	Risk level after actions taken
1. Xxxxxx; xxxxxx	Minimal / Low	xxxxxx	Low
2. xxxxxx; xxxxxx	Some / Medium	xxxxxx	Low
3. xxxxxx; xxxxxx	Serious / High	xxxxxx	Medium

Use a risk matrix

The following matrix may be useful when assessing the *level of impact; likelihood of the risk* and the *risk level after the actions* are taken to reduce or eliminate the risks. You should aim to achieve a **Low** score. This means the proposed activity is unlikely to breach the data protection legislation. If it comes out as **Medium**, see if there is anything further you can do to reduce the likelihood of the risk occurring. If you can't reduce this level, then you will need to decide whether this risk is acceptable.

Level of Impact				
Minimal Impact	**Some Impact**	**Serious Impact**		
Medium	**High**	**High**	**Likely**	**Likelihood of risk occurring after actions are taken**
Low	**Medium**	**High**	**Possible**	
Low	**Low**	**Medium**	**Remote**	

If your assessment comes out as **High** and you cannot put in place any other mitigations to reduce this rating, then your proposed activity **should not go ahead** unless this is approved by the Information Commissioner. Further information about this can be found on the Information Commissioner's website at www.ico.gov.uk

Your Data Protection Officer will seek approval in such cases or advise what else you can do to reduce the risk to a low or medium level.

Contact your Data Protection Officer Amber Badley for advice and support

Email: DPO@firebirdltd.co.uk

www.firebirdltd.co.uk