

Data Protection Impact Assessments (DPIAs): When and How

A Data Protection Impact Assessment (DPIA) is an important process you must understand if your startup handles personal data, especially if you monitor individuals or process particularly sensitive information.

At its core, a DPIA is a structured way to identify, assess, and reduce risks connected with your usage of information about individuals, such as customers, employees, or users. Legally, the requirement to carry out a DPIA comes from the General Data Protection Regulation (GDPR), stating that it must be performed whenever your planned data processing is likely to result in a high risk to the rights and freedoms of natural persons. Typical examples that create these high risks include using artificial intelligence, managing large sets of user data, handling sensitive medical, financial, or biometric information, and making decisions about individuals exclusively by automated means.

Besides compliance with the GDPR, DPIAs can also help you identify data protection issues before they lead to problems and demonstrate regulators that you analyzed your processing activities and mitigated potential risks. They also show investors and customers that your business takes data protection seriously, especially in more sensitive sectors, such as MedTech.

Therefore, in this post we will describe the main steps you need to look into when assessing if you need to conduct a DPIA and, if so, how to start.

When are DPIAs required?

To know if you need to complete a DPIA, you first need to understand if your processing activities raise a risk towards individuals, and if so, how severe that harm could be. Think about how your data processing could have a negative impact on people, whether financially, reputationally, or i.e. by affecting their access to services or employment. There are some questions you can ask yourself to get an idea of the level of risk your processing entails:

1. Do you use innovative technologies (AI, facial recognition, etc.)?
2. Do you process data about vulnerable individuals, such as children?

3. Do you combine or match personal data from different sources?
4. How intrusive is your processing and how many people may be affected?

However, and given their intrusiveness and risk, the GDPR sets out three specific processing situations where a DPIA is always required:

1. **Systematic and extensive profiling with significant effects:** This means processing, especially automatically, where outcomes can have legal consequences or other major impacts on people (for example, software making decisions on whether someone receives a loan or is hired for a job).
2. **Large-scale processing of special category data:** These are particularly sensitive personal data, such as health, genetic, or biometric information, processed on a broad scale.
3. **Systematic monitoring of public areas at large scale:** For instance, video surveillance covering public spaces, which could track individuals' movements.

If in doubt, it's safer to conduct a DPIA. You'll both future-proof your business and build customer confidence by demonstrating responsible data management from the start.

How to draft a DPIA

After concluding that you need to conduct a DPIA, the next step is to do it. Here's a quick guide on the main steps you need to take:

1. **Map your processing activities.** Map how personal data moves through your system's, from collection to deletion. Document what data you collect, the reason for collecting it, applicable legal bases, who can access it, how long you will keep it, and whether it leaves your organization (and, if yes, where). Be thorough: this first step is critical for you to have all the information you need to conduct a strong risk assessment for the processing activities you want to start.
2. **Assess the necessity and proportionality of your processing.** This means asking whether you need to collect all the personal data you plan to, or can you achieve

your goals with less. It also means asking for how long you need to store that information and adopting policies to minimize its retention and access.

3. **Identify and assess the risks to individuals' rights and freedoms.** Consider possible adverse effects to what you are planning to do: unauthorized access, data breaches, discrimination from automated decisions, loss of control, etc. The most effective way to prioritize and address these risks is through a risk matrix, mapping each risk by its likelihood of happening against the severity of its potential impact. For every risk identified, ask: how likely is this event, and how damaging would it be for individuals if it happened?
4. **Identify measures to mitigate identified risks.** For all medium or high risks, set out specific safeguards. Technical safeguards are your frontline defense. Encrypt data both when stored (at rest) and when being transmitted (in transit). Use pseudonymization to swap identifiable information for pseudonyms or codes. Organizational measures work together with these technical ones. Sign data processing agreements with every third party that handles personal data. Train your team regularly on your data protection policies and legal duties, as human error is a common root cause of data breaches. For each safeguard, record its impact on the risk and weigh up the implementation cost versus the risk reduction provided.
5. **Consult with stakeholders and individuals.** It is also important to engage with relevant parties early on. If you have a Data Protection Officer (DPO), their input is crucial, so document their advice. Include technical teams to clarify security risks, legal advisors for compliance, and data processors for a complete operational perspective. When possible, seek the opinions of individuals whose personal data is involved, or engage with their representatives. If you decide against their suggestions, record your reasons for transparency.
6. **Record outcomes and have final consultations.** Summarize all findings in your DPIA. Include each risk, its severity, proposed mitigation, and any residual risks you foresee remaining after actions are taken. Obtain written advice and sign-off from your DPO and management and, if any high risks remain after mitigation, you must consult your supervisory authority before starting processing.

What to do after conducting the DPIA

Once your DPIA is done, you still need to pay attention to some elements. For example, a DPIA should not be static. Your technology, products, and regulatory environment evolve, so your DPIA needs updates to stay relevant. This means that you should record when the initial DPIA was completed, and set up a schedule for reviews, for example, whenever you change your processing operations, introduce new tools, or face new regulatory guidance.

Secondly, it is important to apply your DPIA findings directly into your projects. Assign recommended mitigation actions to owners with clear deadlines. Assign governance responsibility, ideally to your DPO, or if you don't have one, to another specific team member. Lastly, don't forget that, especially in regulated sectors, transparency can boost trust. While publication isn't required, consider how sharing your DPIA (with sensitive details withheld) with stakeholders can enhance your reputation.


Francisco Argã e Lima

December 2025

Paxlegal

 paxlegal@paxlegal.pt

 www.paxlegal.pt

 Av. Eng. Duarte Pacheco, Torre 1
14.º andar – Sala 1
1070-101 Lisboa, Portugal