Webster UNIVERSITY

Office of Privacy

# Data Protection Impact Assessment (DPIA) Explained

September 2021

# Table of Contents

## Webster University Privacy Program Mission

The mission of the **Office of Privacy** is to protect both personal and sensitive information promoting transparency for prospective students, current students, faculty, adjunct faculty, alumni, employees and all other constituents of Webster University. We work diligently to preserve individuals' privacy. We strive to be a valued partner and adviser to the entire University community, to protect the integrity of data collected, created, transmitted, released, stored and otherwise processed by Webster University.

We view privacy compliance as a responsibility of all constituents of the University community and work toward implementing the appropriate systems and structures to provide all employees and business units' support, advice and guidance to assure that ethical and regulatory requirements are identified and met.

We adhere to the regulatory requirements governing our organization and we work to ensure privacy compliance with all sovereign, federal, and state agencies as well as with all accrediting agencies/regulators. We strive to meet or exceed industry standards and best practices.

For questions or for further information, please contact:

**Jeanelle Wiley**
University Secretary and Webster Senior Privacy Director
+13142467123
privacy@webster.edu

**Edna Schick-Bodrič**
Director of Privacy Governance and Programs, International Campuses
+43126992934334
privacy@webster.ac.at

**Ellie Despotaki**
Data Privacy Operations Manager, International Campuses
+302119905302
privacy@webster.edu

## What is a Data Protection Impact Assessment?

**Data Protection Impact Assessment (DPIA) is a process for building and demonstrating compliance**.

A DPIA is a direct consequence of the **accountability principle of the General Data Privacy Regulations (GDPR)**. An organization is accountable for demonstrating that it has taken all of the measures necessary to ensure compliance with the GDPR.

**Data controllers** should see carrying out a DPIA as a useful and positive activity that aids legal compliance.

A DPIA is required whenever **processing is likely to result in a high risk to the rights and freedoms of individuals**.

The DPIA should be **conducted before the processing** and should be considered as a living tool, not merely as a one-off exercise. Where there are residual risks that can't be mitigated by the measures put in place, the Data Protection Authority (DPA) must be consulted prior to the start of the processing.

## What does 'high risk' mean?

**Risk in this context is about the potential for any significant physical, material or non-material harm to individuals.**

To assess whether something is 'high risk', the GDPR is clear that both likelihood and severity of any potential harm to individuals have to be considered. '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 task 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?** The screening is done for any red flags which indicate that a DPIA needs to be done and to look at the risk (including the likelihood and severity of potential harm) in more detail.

## When is a DPIA required?

If the **processing activity meets at least two of the following criteria**, then it is required to perform a DPIA.

1. **Innovative use and/or applying new technological or organizational solutions** (e.g. IoT applications, AI, facial recognition, etc.);
2. **Evaluation or scoring, including profiling and predicting**, especially from "aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behavior, location or movements" (e.g., behavioral profiling, most segmentation techniques used for marketing purposes);
3. **Automated decision-making with a legal or similar significant effect**;
4. **Systematic monitoring**;
5. **Sensitive data or data of a highly personal nature** (e.g., health data, trade union membership, genetic data, etc.);
6. **Data processed on a large scale**;
   Note: Although there is no clear definition of what constitutes 'large scale', the Article 29 Working Party advises taking the following criteria into account:
   a. the number of data subjects concerned, either as a specific number or as a proportion of the relevant population;
   b. the volume of data and/or the range of different data items being processed;
   c. the duration, or permanence, of the data-processing activity;
   d. the geographical extent of the processing activity.
7. **Matching or combining datasets** (e.g. data enrichments that might be carried out prior to a marketing campaigns)
8. **Data concerning vulnerable data subjects**.

**Note**: 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**.

9. When the processing in itself "prevents data subjects from exercising a right or using a service or a contract". Data that is being processed is necessary to evaluate the possibility of offering services or products (e.g., the processing of health data by an insurance company before entering into an insurance on outstanding balance).

## What are the steps for conducting a DPIA?

- 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

## DPIA Checklist Template and Pre-Screening Questions

In case a business unit/department/unit/function at Webster University is proposing to introduce a new business activity or data processing solution where the new service(s) will involve the processing of personal data, **Webster University DPIA Checklist Template and Pre-Screening Questions will need to be completed**. As Data Controller for our employee, student and business contact data Webster University is required to perform and document a data protection impact assessment (DPIA) for the University´s internal processing. A DPIA is an assessment of "the necessity and proportionality of the processing" and "the impact to the rights and freedoms of individuals over the processing of their personal data". A DPIA is also required when new technologies are introduced and when existing personal data will be used for new purposes.

**Project managers (or business sponsors) are required to complete and submit this assessment to:**

eschickbodric73@webster.edu

and

privacy@webster.edu

## Further GDPR and DPIA Resources

- Webster University Office of Privacy
- European Data Protection Board
- General Data Protection Regulation Articles and Recitals
- Information Commissioner's Office
- The International Association of Privacy Professionals