GDPRism

Template:
Third-party provider audit

This template supports the data protection risk assessment of a third-party provider or service provider.

Important: This information sheet does not constitute legal advice. The contents do not claim to be complete and are not guaranteed. It merely serves as an introduction and provides an initial overview of data protection regulations.

Details of the service provider

Which service, internet service or service provider is it?

Where is the service provider based? (Please enter address)

Part I. Examination of the risk

Intended use

What is the service, internet service or service provider to be used for? What is the use case or purpose of the service?

Risk assessment Operation

How high do you rate the risk of using the provider? Please assess the impact on your own business if the service were to fail and no longer be available.

Low risk	**Medium risk**	**High risk**
The unavailability of the software does not pose a significant risk to operations. A failure of the application has no lasting effects	The application is important for business operations. A failure could hinder or negatively impact operations in the short term, but without lasting effects.	A failure of the system would have an extreme impact on business operations. The system is important for maintaining key functions. A failure would lead to direct costs.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Threshold value analysis - Possible harm to the persons concerned

In risk management, a risk basically has two dimensions: Firstly, the severity of the loss and secondly, the likelihood of the event and consequential losses occurring.

Evaluate the potential risk using the table below.

Severity of the damage				
Maximum				
Essential				
Limited		X		
Negligible				
	Negligible	Limited	Essential	Maximum
	Probability of occurrence			

Severity of the damage:

- **Negligible:** Those affected may suffer inconvenience, but they can overcome this with a few problems.
- **Limited**: Those affected may experience significant discomfort, which they can overcome with some difficulty.
- **Essential**: Those affected may suffer significant consequences that they can only overcome with serious difficulties.
- **Maximum**: Those affected may suffer significant or even irreversible consequences that they cannot overcome.

Probability of occurrence:

- **Negligible:** Based on current expectations, no damage can occur.
- **Limited**: Damage may occur, but based on experience to date and the prevailing circumstances, this seems unlikely.
- **Significant**: Based on previous experience and the given circumstances, the occurrence of damage appears possible but not very likely.
- **Maximum**: The occurrence of damage appears to be possible and highly probable based on experience to date and the given circumstances.

Source:
Document "Risk analysis and data protection impact assessment" by the Bavarian State Commissioner for Data Protection

Part II Provider check

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

GDPRism

Access by the provider

What kind of service is it? Is it software that is installed locally or via an Internet application?

In the case of an Internet application: Does the provider have remote access to the user in case of maintenance?

Yes	**no**	**unclear**

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Checking third country reference

If personal data is transferred to a third country, the corresponding destination country must be identified and checked. This can be done using the following country categories:

- **Countries without significant risks:** EU countries and all countries for which an adequacy decision has been adopted by the EU (including Norway, Liechtenstein, Iceland, Andorra, Argentina, Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, Canada, New Zealand, Switzerland, Uruguay, UK, USA)
- **Risky countries:** Countries that are not included in the list of countries without significant risks.
- **Critical countries:** Critical countries include China, India and countries without rule-of-law structures.

Where is the service provider based?

Countries without significant risks	**Countries at risk**	**Critical countries**

Is there a parent company and if so, where is it based?

Countries without significant risks	**Countries at risk**	**Critical countries**

Does the service provider use subcontractors based in one of the country classes?

Countries without significant risks	**Countries at risk**	**Critical countries**

In which country does the data processing take place?

Countries without significant risks	**Countries at risk**	**Critical countries**

Examination of contractual obligations

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Does the provider provide comprehensive information about its data protection and IT security-related activities?

Yes	**no**	**unclear**

Does the provider offer an AV contract? Only relevant if it is a classic order processing.

Yes	**no**	**unclear**

Co-funded by the European Union

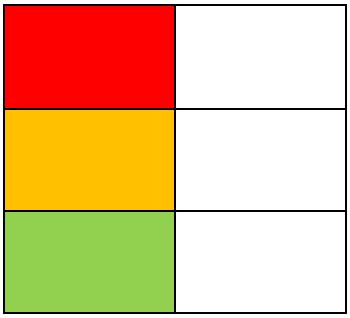
Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

GDPRism

Part III Final assessment

Risk categorisation

Make a note of how often you selected answer options of the corresponding colour in this questionnaire:



If you have selected fields marked in **RED**, you should urgently seek data protection advice before using the service provider.

If you have selected fields marked **ORANGE**, you should check the use of the service provider in detail. The marked areas should be checked again and, if necessary, clarified directly with the service provider. The use of the service provider is at least risky. It may be necessary to carry out a separate risk assessment or further checks.

All fields marked **GREEN** represent "normal" risks. This does not mean that the use of the service provider is absolutely risk-free. When using the service, you as the controller must nevertheless take appropriate technical and organisational measures to ensure that the data is processed in accordance with data protection law.

Conclusion / Measures

Carry out a final assessment based on the information provided. Describe what measures you plan to take to minimise any identified risks or to examine them further in detail.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.