Third-Party Risk Management: good practices according to EU legislation (*GDPR, NIS2, Data Governance Act & DORA*)

Keller & Heckman

The below checklist of **good practices regarding third-party risk management** is based on **statutory requirements** according to four pieces of EU legislation: the General Data Protection Regulation (GDPR), the NIS2 Directive, the Data Governance Act, and the Digital Operational Resilience Act (DORA). It is not a comprehensive list of good practices for third-party risk management (or of statutory requirements), but it highlights many good reflexes to have.

Integrate it in your flow, improve it, and share your own list with us!

Examples of good practices for TPRM

- ☐ **Due diligence:** Only select providers capable of enabling legal compliance.[1]
- ☐ **Contract:** Conclude a contract or similar binding legal instrument with your provider.[2]
- ☐ **Restrictions to provider's freedom:** Consider what the provider should be permitted to do with your data.[3]
- ☐ **Confidentiality:** Require confidentiality both during the relationship (through non-disclosure)[4] and afterwards (through return and then destruction of data on the provider's end).[5]
- ☐ **Security:** Ensure that the provider has implemented appropriate security measures (technical measures as well as organisational ones)[6] and that the provider provides rapid and sufficient information regarding any security incident.[7]
- ☐ **Interactions with third parties:** Determine the level of assistance you may need from the provider in case of requests from or interactions with third parties (users, regulators).[8]
- ☐ **Evidence collection:** Collect from your provider any information that enables you to document compliance with both the contract and the law, for instance by way of audits or information requests.[9]
- ☐ **Cascading obligations:** Ensure that contractual requirements are reflected in subsequent relationships where relevant (e.g., confidentiality also for provider's employees).[10]
- ☐ **Stakeholder involvement:** Ensure all relevant levels are properly informed and involved in the relevant strategy (e.g., cybersecurity strategy), including management and the Board of Directors.[11]
- ☐ **Auditing re-use:** If you allow re-use of data under certain conditions, consider how to verify in practice that the recipient complies with those conditions.[12]
- ☐ **Safeguarding de-identification:** Where information is being provided in a pseudonymised form, consider:
  - a contractual prohibition of reidentification,
  - organisational measures to prevent sharing information enabling reidentification, and
  - technical measures to further reduce the risk of reidentification.[13]
- ☐ **Beyond data rules:** Do not limit yourself to verifying compliance with data-related legislation but also consider e.g., intellectual property laws.[14]
- ☐ **Review your strategy:** Adopt and regularly review your strategy on third-party risk, including a multi-vendor strategy as appropriate.[15]
- ☐ **Contract management:** Maintain information on your contractual arrangements with service providers.[16]
- ☐ **Auditor skillset:** Ensure that any auditors, whether internal or external, possess appropriate skills and knowledge to effectively perform the relevant audits and assessments, in particular in case of high technical complexity of the services audited.[17]
- ☐ **Exit strategy:** Consider the scenarios for termination of the relationship with the service provider and the consequences, so that you are able to exit without:
  - disruption to your business activities,
  - hindering legal compliance, and
  - detriment to service continuity & quality.[18]
- ☐ **Assess substitutability:** When evaluating a possible service provider, take into account whether this would lead to contracting a service provider that is not easily substitutable or that concentrates too many critical or important functions, and if so, weigh the benefits and costs of alternatives.[19]
- ☐ **Know location:** Identify where the services are provided and where the data is processed.[20]

Some concepts can be found in various laws (such as the general requirements regarding confidentiality & security). These footnotes only include references to one statutory source, to keep this document light.

[1] See Art. 28(1) of the General Data Protection Regulation / GDPR (Regulation (EU) 2016/679).
[2] Art. 28(3) GDPR.
[3] Art. 28(3)(a) GDPR.
[4] Pursuant to Art. 28(3)(b) GDPR.
[5] Art. 28(3)(g) GDPR.
[6] Art. 28(3)(c) GDPR refers to Art. 32 GDPR.
[7] Art. 33(2) and 28(3)(f) GDPR.
[8] Art. 28(3)(e) and (f) GDPR.
[9] Art. 28(3)(h) GDPR.
[10] Regarding employees, see Art. 28(3)(b) GDPR and endnote 4 above. Regarding sub-contractors, see Art. 28(2), 28(3)(d), and 28(4) GDPR.
[11] Art. 20 (1) of the NIS2 Directive (Directive (EU) 2022/2555).
[12] Art. 5(4) Data Governance Act (Regulation (EU) 2022/868).
[13] Art. 5(5) Data Governance Act.
[14] See Art. 5(7), 5(8), and 5(10) DGA.
[15] See Art. 28(2) DORA (Regulation (EU) 2022/2554).
[16] Art. 28(3) DORA.
[17] Art. 28(6) DORA.
[18] Art. 28(7) and (8) DORA.
[19] Art. 29(1) DORA.
[20] Art. 30(2)(b) DORA.