7 Elements Every DPA Should Have: A Handy Checklist

GDPR imposes a number of obligations on companies that collect and use personal data. One of the most important of them is the duty to sign a data processing agreement (DPA) with every business partner they share this data with. A DPA is a document that ensures that both data processors and data controllers understand their role in the process and the obligations they take on.

Sounds good, but what about the details? First, a short disclaimer: we're not lawyers and the requirements of a particular DPA can vary from business to business. But based on the text of the regulation and our own experience, we've prepared a checklist of elements every data processing agreement should have. Let's have a look:

1) **General clauses** – you need to provide definitions of the terms used in the document, namely:

- ☐ The object of the agreement
- ☐ The scope, nature, and duration of data processing
- ☐ Data processing subjects
- ☐ Types of processed data
- ☐ Location of data storage
- ☐ Terms of the contract and conditions for its termination

2) **Rights and responsibilities of data controllers** – here you list the duties of the data controller, including:

- ☐ Responsibility for establishing a lawful data management process and observing the rights of data subjects
- ☐ Responsibility for issuing instructions on data processing - a note that the data processor must handle the data in full compliance with the controller's instructions

3) **Responsibilities of data processors** – in these clauses you cover the most important duties of the data processor. According to the law, they should:

- [ ] Have adequate information security measures in place
- [ ] Not engage sub-processors without the prior consent of the controller
- [ ] Cooperate with the authorities in the case of an enquiry or audit
- [ ] Report data breaches to the controller without undue delay (establish time limits)
- [ ] Disclose the name and contact details of their Data Processing Officer
- [ ] Give the data controller the opportunity to conduct audits examining their GDPR compliance (determine the frequency and exact circumstances)
- [ ] Keep records of all processing activities
- [ ] Comply with EU transborder data transfer rules (if necessary)
- [ ] Help the controller to comply with data subjects' rights (including the processing of data subject requests)
- [ ] Assist the data controller in managing the consequences of data breaches
- [ ] Delete or return all personal data at the end of the contract at the choice of the controller

A piece of advice: Make sure that the text of your DPAs doesn't leave any room for misinterpretation! Data processors should know exactly what is expected of them.

4) **Technical and organizational measures** – this is a list of requirements the data processor has to meet in order to satisfy the provisions of GDPR. Among other things, you should include instructions to the effect that:

- [ ] The processor should implement all technical and organizational measures before starting to process users' personal data

Due to the complexity of these measures, it's best to detail them in an annex to the DPA (see: **Annex 1**).

5) **Sub-contractual relationships** – this is a description of the relationship between the primary data processor and sub-processors. Include here instructions that the data processor should:

- [ ] Obtain the written consent of the data controller to establish any kind of relationship with sub-processors
- [ ] Ensure a level of data protection comparable to that provided by a DPA
- [ ] Be responsible for verifying sub-processors' compliance on a regular basis (for instance, at least once every 12 months)
- [ ] List the sub-processors in a separate annex to the agreement (see: **Annex 2**)

6) **Final clauses** – to leave no room for misinterpretation, it's worth adding that:

- [ ] Any changes to the contract must be accepted by both parties
- [ ] The DPA supersedes all other agreements between the data processor and data controller

7) **Annexes** – these complement and elaborate contractual arrangements.

Annex 1– Technical and organizational measures. In this part the data processor should prove they're prepared to handle data properly. Make sure they provide details about the following measures:

Confidentiality:

- ☐ The structure of the data center where they plan to store personal data
- ☐ Information security control protocols
- ☐ Physical access to the office and applied security measures
- ☐ Remote access to the office
- ☐ Access control for applications (software)

Integrity:

- ☐ Measures taken to ensure that personal data can't be read, copied, altered, or removed by any unauthorized party during data transfers

Availability & resilience:

- ☐ A detailed description of backup policies, as well as measures used to ensure data redundancy, recoverability, and high availability

Procedures of periodic review:

- ☐ A framework for periodic evaluation of technical and organizational measures presented in the previous parts of the annex

Annex 2 – List of sub-processors. Remember to include their full names and addresses!