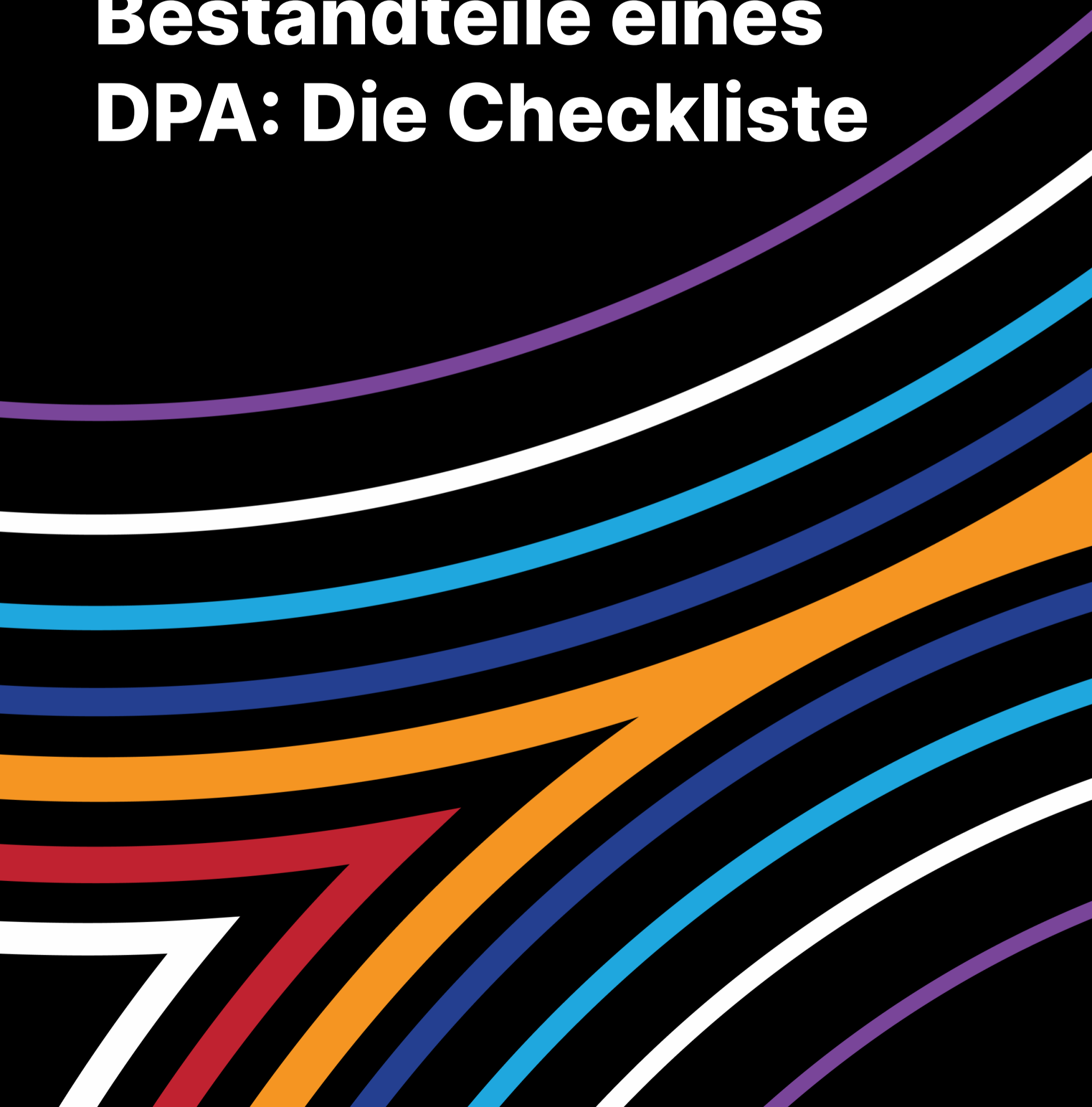


PIWIK **PRO**

Die sieben wichtigsten Bestandteile eines DPA: Die Checkliste



Die DSGVO verpflichtet Unternehmen, die personenbezogene Daten erheben und verwalten, zu einer Reihe von Aufgaben. Eine der wichtigsten ist, einen Data Processing Agreement (DPA), also einen Auftragsverarbeitungsvertrag (AVV), mit jedem Geschäftspartner zu unterzeichnen, mit dem sie diese Daten teilen. Das Dokument stellt sicher, dass sowohl der Datenverarbeiter als auch der Datenverantwortliche ihre Aufgaben und Pflichten verstehen.

Klingt gut, aber wie sieht es im Detail aus? Zuerst ein kurzer Haftungsausschluss: Wir sind keine Juristen. Dies gesagt, Vorgaben für bestimmte DPAs weichen je nach Unternehmen voneinander ab. Wir stützten uns an die Verordnung und unsere Erfahrung, und erstellten eine Checkliste mit den wichtigsten Bestandteilen eines DPA.

1) Generelle Klauseln – Definieren Sie Begriffe, die Sie im Dokument verwenden:

- Vertragsgegenstand
- Umfang, Art und Dauer der Datenverarbeitung
- Betroffene Personen der Datenverarbeitung
- Datentypen, die verarbeitet werden
- Ort der Datenspeicherung
- Vertragslaufzeit und Bedingungen bei Vertragsbeendigung

2) Rechte und Pflichten des Datenverantwortlichen – Listen Sie auf, wofür der Datenverantwortliche zuständig ist:

- Der Datenverwaltungsprozess ist gesetzeskonform einzurichten und die Rechte betroffener Personen müssen beachtet werden.
- Die Datenverarbeitung vorgeben. Hinweis, der Datenverarbeiter muss die Daten in vollem Einklang mit den Richtlinien des Datenverantwortlichen handhaben.

3) Pflichten des Datenverarbeiters – Decken Sie in diesen Klauseln die wichtigsten Ansprüche an den Datenverarbeiter ab. Der Datenverarbeiter:

- Verfügt über geeignete Maßnahmen zur Informationssicherheit
- Darf keinen weiteren Datenverarbeiter beteiligen, ohne vorheriger schriftlicher Genehmigung des Datenverantwortlichen
- Arbeitet im Fall einer Anfrage oder Prüfung mit den Behörden zusammen
- Meldet unverzüglich jegliche Datenschutzverletzungen (legen Sie Fristen fest)
- Gibt den Namen und die Kontaktdaten seines Datenschutzbeauftragten bekannt
- Ermöglicht dem Datenverantwortlichen die Prüfung seiner DSGVO-Compliance (bestimmen Sie, wie oft und unter welchen Umständen dies geschieht)
- Dokumentiert alle Verarbeitungsaktivitäten
- Befolgt die europäischen Vorschriften für den grenzüberschreitenden Datentransfer (falls erforderlich)
- Unterstützt den Datenverantwortlichen, die Rechte und Freiheiten betroffener Personen zu schützen (einschließlich der Verarbeitung von Datenschutzanfragen)
- Unterstützt den Datenverantwortlichen die Folgen einer Datenschutzverletzung zu bewältigen
- Löscht bei Vertragsende die Daten oder retourniert alle personenbezogenen Daten (je nach Wahl des Datenverantwortlichen)

Hinweis: Stellen Sie sicher, dass der Text Ihres DPA keinen Platz für Fehlinterpretation lässt! Der Datenverarbeiter soll genau wissen, was Sie von ihm erwarten.

4) Technische und organisatorische Maßnahmen – Anforderungen, die der Datenverarbeiter erfüllen muss, um Daten gemäß der DSGVO zu schützen:

- Der Datenverarbeiter setzt alle technischen und organisatorischen Maßnahmen um, bevor die Verwaltung personenbezogener Daten beginnt.

Aufgrund der Vielfalt dieser Maßnahmen empfehlen wir, die Anforderungen im Anhang des DPA zu beschreiben (siehe: **Anlage 1**).

5) Untervertragsverhältnisse – Anforderungen, die die Zusammenarbeit zwischen dem primären Datenverarbeiter und einem weiteren Datenverarbeiter, im weiteren Untervertrag, darstellen. Der primäre Datenverarbeiter soll:

- Die schriftliche Einwilligung des Datenverantwortlichen einholen, bevor ein Untervertragspartner beauftragt wird
- Ein Maß an Datenschutz gewährleisten, das der Datenschutzebene in dem gesetzten DPA vergleichbar ist
- Die Compliance seitens Untervertragspartner regelmäßig überprüfen (z. B. mindestens einmal alle 12 Monate)
- Dem Vertrag alle Untervertragspartner in einer separaten Anlage beilegen (siehe: **Anlage 2**)

6) Schlussklausel – lassen Sie keinen Raum für Fehlinterpretationen:

- Jegliche Vertragsänderungen müssen von beiden Parteien akzeptiert werden
- Der DPA hebt alle anderen Vereinbarungen zwischen dem Datenverarbeiter und Datenverantwortlichen auf

7) Anlagen – diese ergänzen und erläutern den Vertrag.

Anlage 1 – Technische und organisatorische Maßnahmen. In diesem Teil sollte der Datenverarbeiter beweisen, Daten angemessen verarbeiten zu können.

Vertraulichkeit:

- Die Struktur des Rechenzentrums, das personenbezogene Daten speichern soll
- Kontrollprotokolle zur Informationssicherheit
- Physischer Zugang zum Büro und angewandte Sicherheitsmaßnahmen
- Fernzugriff auf das Büro
- Zugriffskontrolle für Applikationen (Software)

Integrität:

- Maßnahmen, die sicherstellen, dass personenbezogene Daten von Unbefugten nicht gelesen, kopiert, verändert oder während eines Datentransfers gelöscht werden

Verfügbarkeit und Belastbarkeit:

- Eine ausführliche Beschreibung der Backup-Richtlinien sowie der Maßnahmen zur Sicherung der Datenredundanz, Wiederherstellbarkeit und hoher Verfügbarkeit

Verfahren zur regelmäßigen Überprüfung:

- Ein Rahmen für das periodische Auswerten von technischen und organisatorischen Maßnahmen, die in den vorigen Teilen des Anhangs vorgestellt wurden

Anlage 2 – Liste der Untervertragspartner. Vergewissern Sie sich, dass die Liste den vollständigen Namen und Adresse der Beteiligten beinhaltet!

Sie suchen nach einer idealen Analytics Plattform?

Nutzen Sie den kostenlosen Core Plan und legen Sie los. Sie benötigen mehr?
Vereinbaren Sie eine Demo Ihrer idealen Piwik PRO Konfiguration.

Individuelle Piwik PRO Demo

Kostenlose Core Instanz

Über Piwik PRO

Piwik PRO ist eine Datenschutz-konforme Plattform, die fortgeschrittene, aus Google Analytics bekannte, Analytics Features anbietet und dabei komplette Datenkontrolle zulässt. Diverse Organisationen nutzen Piwik PRO wegen der leistungsfähigen, Datenschutz-konformen Analytics-Software und den eminenten Kundendienst. Die Deutsche Flugsicherung, die Europäische Kommission und Greiner verwenden Piwik PRO, um ihre Customer und User Journey zu optimieren. Die Features und Hosting Optionen der Piwik PRO Analytics Suite erlauben dessen Nutzung in anspruchsvollen Umgebungen, um interne Sicherheits- und Rechtsverordnungen zu befolgen, sowie auch Datenschutzverordnungen zu respektieren, wie zum Beispiel die DSGVO, die CNIL und die CCPA.

Kontakt

EMEA

+48 71 716 69 50

DACH

+49 2203 989 620

BENELUX

+31 858 881 458

NORD AMERICA

+1 (888) 444 0049