Tabellarische Übersicht wichtiger Nachweispflichten

Konkrete Vorgaben an die Art des Nachweises stellt die DSGVO nicht. In welcher Form die Datenschutzdokumentation geführt wird, bleibt dem Verantwortlichen vorbehalten. Er entscheidet daher selbst, wie die Erstellung und Verwaltung von Datenschutzdokumenten zu erfolgen hat und welche Struktur sie haben sollen. In jedem Fall sollte sich der Aufwand an den Erfordernissen und Verhältnissen des Verantwortlichen ausrichten.

Nach dem Baustein 42 des Standard-Datenschutzmodells der Aufsichtsbehörden sollten folgende Anforderungen eingehalten werden:

Anforderung	**Beschreibung / Umsetzung**
Strukturierung der Gesamtdokumentation	• Gliedern Sie die gesamte Dokumentation in Module.
Dokumentation über elektronischen und in Papierform vorliegenden Teile	• Halten Sie ein aktuelles Backup-Medium für den elektronischen Teil der Dokumentation bereit. Damit können Sie auf die Dokumentation auch im Fall eines Systemausfalls zugreifen. • Dokumentieren Sie auf Papier, wie bei einem Ausfall der IT zu verfahren ist, z. B. ein Verweis auf den Standort eines gesicherten Backupmediums.
Angemessenheit und Vollständigkeit	• Vermeiden Sie ein Übermaß an Dokumentation. • Nicht angemessen ist der Ausdruck vollständig ausgefüllter Vordrucke oder von Sicherheitsstandards.
Revisionsfestigkeit	• Erstellen Sie Versionierungs- und Fortschreibungsregel, um den Stand der Stand der Dokumentation nachweisen zu können.
Aktualität und Fortschreibung	• Die Dokumentation muss regelmäßig aktualisiert werden.

Grundsätze	Nachweise	Bearbeitungsstatus
1. Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz	(1) Rechtsgrundlagen der Datenverarbeitung • Dokumentation bestehender Verarbeitungsprozesse im Verzeichnis der Verarbeitungstätigkeiten • Festlegung der richtigen Rechtsgrundlage für jede Verarbeitung • Dokumentation eingeholter Einwilligungen (2) Informationspflichten • Protokollierung der übermittelten Informationen an betroffene Personen zur Datenverarbeitung • Erfasste Maßnahmen wie Datenschutzerklärungen, Mitarbeiterhandbücher (Art. 13, 14 DSGVO) (3) Rechte der betroffenen Personen • Information über Rechte wie: Auskunft, Korrektur, Löschung, Einschränkung, Widerspruch, Widerruf der Einwilligung, Rechte bei automatisierten Entscheidungen • Umgesetzte Maßnahmen bei der Geltendmachung dieser Rechte (z.B. Erteilung von Auskünften, Übertragung von Daten, Löschung, Einschränkung, Berichtigung, Bearbeitungsfristen für Anfragen) (4) Automatisierte Entscheidungen mit bedeutenden Auswirkungen auf betroffene Personen • Protokollierung der betreffenden Entscheidungsprozesse und deren Begründungen • Sicherstellung von Einflussmöglichkeiten für betroffene Personen auf den Entscheidungsprozess	
2. Zweckbindung	• Bestimmung des Verarbeitungszwecks zu Beginn der Datenverarbeitung (ggf. im Rahmen des Verzeichnisses der Verarbeitungstätigkeiten) • Bei Zweckänderungen: Festlegung der Rechtsgrundlage für die Änderung, • Falls keine Einwilligung vorliegt; ggf. Hinweis über die Vereinbarkeit des alten und neuen Zwecks sowie Benachrichtigung der Betroffenen über den neuen Zweck	

3. Datensparsamkeit	Umgesetzte Maßnahmen zur Datenminimierung, insbesondere Privacy by Design und by Default (z.B. Verschlüsselung, Pseudonymisierung, datensparsame Voreinstellungen)	
4. Richtigkeit	Vorkehrungen zur Gewährleistung der Aktualität und Richtigkeit personenbezogener Daten	
5. Speicherbegrenzung	• Löschkonzept • Implementierung des Löschkonzepts • Durchgeführte Löschungen	
6. Integrität und Vertraulichkeit	• bestehende technische und organisatorische Sicherheitsmaßnahmen (z.B. Notfallmaßnahmen, Sicherungsmaßnahmen für IT-Systeme, Rollen- und Zugriffsbeschränkungen)	
7. Verantwortungsbereiche	• Datenschutzbeauftragter (Eignung und Vertrauenswürdigkeit, Ernennung, ordnungsgemäße Integration und Ausstattung) • Weitere Zuständigkeiten (zentrale oder dezentrale Verantwortungsstruktur)	
8. Organisation des Datenschutzes	• Einführung von Leitlinie für den Datenschutz • Datenschutzrichtlinie und -prozessen	
9. Weitergaben von Daten an Dritte	a) <u>Auftragsverarbeitungsverhältnisse</u> • Nachweis der Auswahl eines zuverlässigen Anbieters (Sicherstellung angemessener technischer und organisatorischer Maßnahmen, um DSGVO-Konformität und Schutz der Betroffenenrechte zu gewährleisten) • Abschluss geeigneter Vereinbarungen zur Auftragsverarbeitung • Protokollierung erteilter Anweisungen • Regelmäßige Überprüfung des Anbieters, z.B. durch Inspektionen vor Ort oder Analyse von Prüfberichten • Umgang mit Vertragsverletzungen und Datenschutzverstößen a) <u>Datenweitergabe an Dritte</u> • Überlegungen zur Zulässigkeit der Weitergabe • Gegebenenfalls Maßnahmen bei gemeinsamen Verantwortlichen	

	b) <u>Gemeinsame Verantwortliche (für einen Verarbeitungsvorgang)</u> • Dokumentation der Zuständigkeitsverteilung • Abschluss eines Vertrags für gemeinsame Verantwortliche gemäß Art. 26 DSGVO c) <u>Internationale Datenübermittlungen (außerhalb der EU)</u> • Nachweis geeigneter Schutzgarantien des Empfängers, z.B. durch Angemessenheitsbeschlüsse der EU-Kommission, EU-Standardvertragsklauseln, Privacy Shield oder entsprechende Zertifizierungen	
10. Verzeichnis über Verarbeitungstätigkeiten	• Verzeichnisses von Verarbeitungstätigkeiten • Regelmäßige Aktualisierung des Verzeichnisses	
11. Schulungen	• Schulungskonzept für Mitarbeiter • Protokollierung durchgeführter Schulungen und Teilnahmebestätigungen	
12. Zusammenarbeit mit den Aufsichtsbehörden	Protokollierung von Kommunikation mit Behörden	
13. Datenpannen	• Handhabung von Datenschutzverletzungen • Mitteilung an Behörden und Betroffene (oder Gründe für das Unterlassen der Benachrichtigung), einschließlich Fristen für Meldungen und mögliche Verzögerungsgründe, falls die Meldung nach mehr als 72 Stunden erfolgt • Maßnahmen zur Abwehr und Schadensminderung	
14. Datenschutzfolgenabschätzungen	• Durchgeführte Schwellwertanalyse • Datenschutzfolgenabschätzungen und deren Aktualisierung bei Bedarf • Gegebenenfalls Erfüllung der Konsultationspflicht gegenüber der Datenschutzbehörde bei hohem Risiko für die Rechte der Betroffenen	
15. Zusammenarbeit mit den Interessenvertretungen	Betriebsvereinbarungen	

16. Regelmäßige Überprüfung der umgesetzten Maßnahmen	• Anpassung der Maßnahmen an neue Vorgaben, Gerichtsurteile oder behördliche Praxis • Protokollierung von Audits und Überprüfungen der Maßnahmen, einschließlich Inhalt und Ergebnis	