Oktober 2026 | Zum Datenschutz aufgefallen



Information zum (Weblink)
Datenschutz - Service
oder Fragen per Mail an:
Mail2@volkerschroer.de

Die Informationen wurden von mir sorgfältig zusammengestellt und beruhen auf öffentlich, zugänglichen Quellen, für die ich keine Gewähr auf Richtigkeit und Vollständigkeit übernehmen kann.
*) Aus Gründen der besseren Lesbarkeit Verwendung der männlichen Form, die alle Geschlechter mit einbezieht.

Liebe(r) Leser(in)*,



Datenschutz → einfach praktisch hilfreich!

Wenn die Grundlagen einmal gelegt, sind die Abläufe meist schlank(er), der Aufwand gering und mit (der) Sicherheit mehr Zeit gewonnen. Datenschutz schafft Vertrauen und ist eine Grundlage für nachhaltigen Erfolg.

Mein Ziel ist es, den Datenschutz einfach, praktisch und hilfreich zu vermitteln und zu gestalten. Von Datenschutzberater, Datenschutzberatung, Datenschutzmanagement bis zertifizierter, externer Datenschutzbeauftragter für Selbstständige, Gewerbetreibende und KMU.

Sprechen wir!

Vielen Dank für Ihr Interesse

PS: Nutzen Sie die Möglichkeit nur zu lesen, was für Sie von Interesse ist, oder kontaktieren Sie mich gerne.

Inhalt

(Einfach interessantes Thema nach Wahl anklicken)

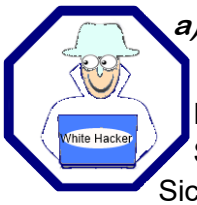
1. Standard – Datenschutz – Modell Vers. 3.1a…1
2. Datenschutz und Datensicherheit…1
a) Penetrationstest (PEN-Test)…1
(1) Erläuterung:…1
(2) Gründe:…1
(3) Ziel:…2
(4) Typische Formen:…2
(5) DS-GVO & PEN-Tests…2
(6) Rechtsgrundlagen…2
(7) Mitarbeiterrechte…2
(8) Schutzmaßnahmen und Vorgaben…2
(9) Vertragliche Regelungen…3
(9.1) Vertragsparteien & Präambel…3
(9.2) Umfang und Begrenzung (Scope)…3
(9.3) Mitwirkungspflichten des Auftraggebers…3
(9.4) Datenschutz & Auftragsverarbeitung (AVV)…3
(9.5) Ergebnisse, Berichtswesen & Re-Test…3
(9.6) Haftung, Vergütung & Laufzeit…3
(10) Vorlagen Muster…3

1. Standard – Datenschutz – Modell Vers. 3.1a

Standard-Datenschutz-Modell *übersichtlich zusammengefasst 11 Seiten*	**Standard-Datenschutz-Modell** Datenschutzkonferenz DSK 78 Seiten	**Datenschutz-Grundverordnung** auf dejure.org	**Bundesdaten-schutzgesetz** auf dejure.org

Das SDM [*der Datenschutzkonferenz der Aufsichtsbehörden des Bundes und der Länder (DSK)*] überführt die rechtlichen Anforderungen der DS-GVO über 7 Gewährleistungsziele in die technischen / organisatorischen Maßnahmen zur Unterstützung der Transformation abstrakter – rechtlicher Anforderungen in konkrete Maßnahmen. Ziel ist, eine gemeinsame Sprache der Juristen und Informatiker für die Verantwortlichen und Datenschutzpraktiker zu finden.
| Aktuell: SDM Version 3.1a (05/2025) Änderung Logo, einzelne grafische Darstellungen, keine inhaltlichen Änderungen
| Letzter Maßnahmenkatalog 11/2021: Nr.51 „Zugriff auf Daten, Systeme und Prozesse regeln."

2. Datenschutz und Datensicherheit



a) Penetrationstest (PEN-Test)

(1) Erläuterung:

Ein PEN-Test (kurz für Penetrationstest[1]) ist ein autorisierter, simulierter Cyberangriff auf ein IT-System, ein Netzwerk oder eine Softwareanwendung. Geleitet wird dieser Test von Sicherheitsexperten (sogenannten PEN-Testern oder „ethischen Hackern"), die Methoden echter Angreifer nutzen, um Schwachstellen aufzuspüren, bevor diese von Kriminellen ausgenutzt werden können.

(2) Gründe:

Für viele Unternehmen sind regelmäßige PEN-Tests vorgeschrieben, um Zertifizierungen wie ISO

1.) *Quelle: https://de.wikipedia.org/wiki/Penetrationstest_(Informatik)*

CC BY SA

27001 oder TISAX zu erfüllen, oder um kritische Infrastrukturen (KRITIS) abzusichern. Offizielle Standards und Prüfangebote stellt unter anderem das BSI (Bundesamt für Sicherheit in der Informationstechnik) bereit[2].

(3) Ziel:

- Aufdecken von Sicherheitslücken, Fehlkonfigurationen oder veralteter Software in einer kontrollierten Umgebung.
- Kein Schaden[3]: Anders als bei echten Angriffen wird das Ziel nicht zerstört oder ausgeraubt; gefundene Lücken werden stattdessen dokumentiert und dem Betreiber gemeldet.
- Abgrenzung zum Schwachstellen-Scanner: Ein automatisierter Scanner sucht nur nach bekannten Mustern. Ein PEN-Test geht weiter, der Tester kombiniert meist manuelle Techniken und Intelligenz, um Lücken aktiv auszunutzen und zu prüfen, wie weit ein Angreifer vordringen könnte.

(4) Typische Formen:

- Externer PEN-Test (Angriff von außen über das Internet)
- Interner PEN-Test (Angriff aus dem Firmennetzwerk heraus)
- Blackbox[4] (Tester wissen fast nichts über das System) vs. Whitebox (Tester bekommen alle Hinterdüfte und Quellcodes offengelegt)

(5) DS-GVO & PEN-Tests

Ein Penetrationstest kann oder muss personenbezogene Daten erreichen, die im System gespeichert oder verarbeitet werden. Daher greift die IT-Sicherheit mit einem PEN-Test in den Datenschutz nach DS-GVO ein. Es muss also eine Regelabsprache geben. In der Regelfall ist kein Auftrags-Verarbeitungs-Vertrag (AVV) erforderlich. Der externe PEN-Tester soll Schwachstellen finden, aber nicht gezielt personenbezogene Daten im Auftrag verarbeiten. Es handelt sich um eine Dienstleistung (Technischer Sicherheitscheck). Die Einsichtnahme in personenbezogene Daten ist dabei ein zufälliger Nebeneffekt (Zufallszugriff). Hier ist kein AVV nach Art.28 DS-GVO erforderlich, sondern ein schriftlicher Auftrag mit Geheimhaltungsvereinbarung. Wenn allerdings der PEN-Tester im Rahmen des Auftrags dauerhaft Zugriff auf personenbezogene Daten hat, diese speichert, kopiert oder bearbeitet, kann eine AVV erforderlich sein.

(6) Rechtsgrundlagen

Ist laut Gesetz eine Penetrationstest vorgeschrieben, z. B. im Finanzsektor über DORA, oder dem Gesetz über das Bundesamt für Sicherheit in der Informationstechnik[5] oder nach dem IT-Sicherheitsrecht der EU-Cybersicherheitsvorschrift (NIS2-Umsetzungsgesetz) ist die rechtliche Grundlage der Art.6 Abs.1c DS-GVO. – ODER - Es besteht ein berechtigtes Interesse des Unternehmens an der Absicherung seiner IT-Infrastruktur und dem Schutz seiner Daten, wie auch aller in- und externen personenbezogenen Daten. Die rechtliche Grundlage dazu ist der Art.6 Abs.1f DS-GVO. Aus meiner Sicht ein echtes, berechtigtes Interesse.

(7) Mitarbeiterrechte[6]

Besteht keine gesetzliche Vorgabe für einen Penetrationstest, ist die Personalvertretung / Betriebsrat zu informieren. Dies gilt im besonderen bei Social-Engineering-Tests, bei dem das Verhalten des Einzelnen sichtbar wird. Bericht über PEN-Tests müssen so anonymisiert werden, dass keine Rückschlüsse auf das Verhalten oder die Leistung einzelner Personen möglich ist.

(8) Schutzmaßnahmen und Vorgaben[7]

- Der PEN-Test darf niemals ohne schriftliche Erlaubnis mit definierten Zielen und Tabubereiche erfolgen, da ansonsten Strafen nach § 202a StGB (Ausspähen von Daten) drohen.
- Nach dem Grundsatz der Datenminimierung, ist nach Möglichkeit mit anonymisierten Testdaten oder in einer Testumgebungen zu arbeiten, um die Verwendung von Echt-Kundendaten zu vermeiden.
- Der Bericht zum PEN-Test ist als Nachweis für die Rechenschaftspflicht nach Art.5 Abs.2 DS-

2.) *Quelle: Bundesamt für Sicherheit in der Informationstechnik: „IS-Penetrationstest und IS-Webcheck“*
3.) *Quelle. https://www.syss.de/leistungen/penetrationstest*
4.) *Quelle: Bundesamt für Sicherheit in der Informationstechnik: Studie PEN-Test*
5.) *Quelle: Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG)*
6.) *Quelle: bytelaw: „Rechtskonforme Penetrationstests: IT-Sicherheit, Datenschutz und die Rolle des Betriebsrats“*
7.) *Quelle: Dr. Datenschutz: „Penetrationstest: Diese Datenschutz-Vorgaben sind zu beachten“*

GVO aufzubewahren (Praxiswert: 3 bis 5 Jahre). Auf den Testsystemen von PEN-Testern versehentlich kopierte echte Daten müssen danach sicher gelöscht werden.

(9) Vertragliche Regelungen

Die nachfolgenden, bereitgestellten Inhalte dienen ausschließlich der allgemeinen Information und Information über die rechtlichen Rahmenbedingungen. Sie stellen keine Rechtsberatung (gemäß dem Rechtsdienstleistungsgesetz – RDG) dar und können eine individuelle, auf den Einzelfall abgestimmte Rechtsberatung durch einen qualifizierten Rechtsanwalt oder eine andere zuständige Stelle nicht ersetzen.

(9.1) Vertragsparteien & Präambel

- Rechtsverbindliche Einwilligung: Die ausdrückliche, schriftliche Erlaubnis des Rechteinhabers der zu prüfenden Systeme.
- Eigentumsnachweis / Befugnis: Bestätigung des Auftraggebers, dass er tatsächlich Eigentümer ist oder die berechtigte Zustimmung des Eigentümers vorliegt.
- Geheimhaltungsvereinbarung (NDA): Schutz vertraulicher Informationen beider Seiten.

(9.2) Umfang und Begrenzung (Scope)

- Genaue Systemabgrenzung: Exakte Benennung von IP-Adressen, URLs, Netzwerken, Anwendungen oder Hardware-Komponenten (Vermeidung von „alles testen“).
- Test-Methodik: Festlegung des Vorgehens (z. B. Blackbox, Greybox oder Whitebox nach BSI-Empfehlung).
- Zeitfenster & Fristen: Exakte Definition von Datum, Uhrzeiten (z. B. außerhalb der Geschäftszeiten) sowie ein klares Ablaufdatum der Genehmigung.

(9.3) Mitwirkungspflichten des Auftraggebers

- Informationsbereitstellung: Rechtzeitige Übergabe von Netzplänen, Zugangsdaten, Dokumentationen oder Sicherheitsrichtlinien (besonders bei Whitebox-Tests).
- Backups: Pflicht des Auftraggebers zu regelmäßigen Datensicherungen (z. B. alle 3 Tage oder direkt vor Testbeginn), da Tests zu Systemausfällen oder Datenverlust führen können.
- Notfall-Kontaktpersonen: Benennung von Ansprechpartnern, die im Ernstfall sofort erreichbar sind, falls ein System abstürzt.

(9.4) Datenschutz & Auftragsverarbeitung (AVV)

- Datenschutzkonformität (DS-GVO): Da PEN-Tester zufällig oder gezielt Einsicht in personenbezogene Daten erlangen können, ist ein Auftragsverarbeitungsvertrag gem. Art. 28 DS-GVO obligatorisch (oft als Anlage integriert).
- Datenlöschung: Klare Regelung, wann und wie temporär erhobene Testdaten oder Logs nach Abschluss des Projekts (z. B. innerhalb von 30 Tagen) gelöscht werden.

(9.5) Ergebnisse, Berichtswesen & Re-Test

- Bericht (Reporting): Art der Dokumentation mit nachvollziehbarer Risikoeinstufung (hoch, mittel, niedrig) und Zusammenfassung - Management.
- Nachbesserung / Re-Test: Ob und in welchem Zeitraum eine erneute Prüfung nach Behebung der Lücken stattfindet.

(9.6) Haftung, Vergütung & Laufzeit

- Haftungsbeschränkung: Regelung für vorhersehbare Schäden und Freistellungsklauseln.
- Vergütung & Fälligkeit: Festpreis oder Aufwandsabrechnung sowie Zahlungsbedingungen (z. B. nach Übergabe des Berichts).
- Kündigung: Fristen für die ordentliche oder außerordentliche Kündigung.
- Anwendbares Recht & Gerichtsstand: Vereinbarung des deutschen Rechts und des Gerichtsstands.

(10) Vorlagen Muster

- Eine sehr ausführliche Vorlage (/Anleitung) stellt der Bundesverband IT-Sicherheit e.V. (TeleTrusT), als größtes Kompetenznetzwerk für die IT-Sicherheit in Deutschland und Europa zur Verfügung. Link: TeleTrusT Handreichung Penetrationstest.
- -Etwas weniger Umfangreiche Vorlagen gibt es im Blog Maisch.law (Dr. Mar Maisch)
- Oder eine schlanke Version unter Datenschutz Guru: Vertrag über die Durchführung eines PEN-Tests.

Bei Bedarf, einfach mal sprechen!