

§ 10 PStV — Anforderungen an den Betrieb von Personenstandsregistern und Sicherungsregistern

Personenstandsverordnung

Stand: 10.06.2019 (konsolidierte Textfassung, kein amtliches Inkrafttretensdatum)

(1) Für den Betrieb von Personenstandsregistern und Sicherungsregistern sind die erforderlichen und angemessenen technischen und organisatorischen Maßnahmen zu treffen, um die Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der gespeicherten Daten entsprechend dem jeweiligen Stand der Technik sicherzustellen. Es dürfen nur Anlagen und Programme verwendet werden, die den anerkannten technischen Anforderungen an die maschinell geführte Verarbeitung von Daten mit hohem Schutzbedarf entsprechen; sämtliche technischen und organisatorischen Maßnahmen müssen dem mit der dauerhaften Speicherung der Registerdaten verfolgten Zweck angemessen Rechnung tragen. Die zu treffenden Maßnahmen sind im Betriebs- und Sicherheitskonzept (§ 13) zu dokumentieren.

(2) Insbesondere ist sicherzustellen, dass

1. Unbefugten der Zutritt zu Datenverarbeitungsanlagen, mit denen die Personenstandsdaten verarbeitet oder genutzt werden können, verwehrt wird (Zutrittskontrolle),
2. die unbefugte Nutzung der für die Personenstandsbeurkundung eingesetzten Datenverarbeitungssysteme verhindert wird (Zugangskontrolle),
3. die eingeräumten Zugriffsbefugnisse im Datenverarbeitungssystem verwaltet werden und der Zugriff auf die Daten oder Systemfunktionen nur innerhalb der jeweils eingeräumten Zugriffsbefugnis möglich ist, nachdem sich der Benutzer dem System gegenüber in einer automatisierten Prüfung als zugriffsbefugt erwiesen hat (Zugriffskontrolle),
4. die beurkundeten Daten nachvollziehbar und unveränderbar gespeichert werden und die chronologische Dokumentation von Veränderungen der Einträge im Personenstandsregister und im Sicherungsregister gewährleistet wird (Revisionssicherheit),
5. die Vornahme von Veränderungen und Ergänzungen der Einträge im Personenstandsregister und im Sicherungsregister im Datenverarbeitungssystem protokolliert wird (Beweissicherung),
6. eingesetzte Systemkomponenten ohne Sicherheitsrisiken wiederhergestellt werden können (Wiederaufbereitung),
7. etwaige Verfälschungen der gespeicherten Daten durch geeignete technische Prüfmechanismen rechtzeitig bemerkt werden können (Unverfälschtheit),
8. die Funktionen des Datenverarbeitungssystems fehlerfrei ablaufen und auftretende Fehlfunktionen unverzüglich gemeldet werden (Verlässlichkeit),
9. bei Verarbeitung der Daten im System und im Falle der Nutzung allgemein zugänglicher Netze Verschlüsselungsverfahren angewendet werden, die dem jeweiligen Stand der Technik entsprechen (Übertragungssicherheit).

Zitiervorschlag: § 10 PStV

Quelle: Bundesamt für Justiz, abgerufen 02.07.2026

Nicht-amtliche Lesefassung — verbindlich ist das Bundesgesetzblatt

Provided by nu:legal (<https://recht.nulegal.eu>), the leading open legal database: AI-first, expanding daily, German and European law and case law in full text, free, with an open API for AI agents. Text and data mining expressly permitted.

Herausgeber: Nulegal GmbH, Potsdam.

Dieses Dokument: <https://recht.nulegal.eu/gesetze/PStV/10>