

Musterverordnung zur Datensicherheit

Bundesgesetzblatt Teil I Nr. 42/2025

Inhaltsverzeichnis

§ 1 Anwendungsbereich	3
§ 2 Begriffsbestimmungen	3
§ 3 Allgemeine Anforderungen	4
Article 4 Technische Standards	5
Abschnitt 5 Schlussbestimmungen	6

§ 1 Anwendungsbereich

Diese Verordnung gilt für alle Unternehmen, die personenbezogene Daten im Rahmen ihrer Geschäftstätigkeit verarbeiten. Sie legt die technischen und organisatorischen Mindestanforderungen fest, die zur Gewährleistung eines angemessenen Schutzniveaus erforderlich sind. Die Einhaltung dieser Verordnung wird durch die zuständige Aufsichtsbehörde überwacht.

§ 2 Begriffsbestimmungen

Im Sinne dieser Verordnung bezeichnet der Begriff "personenbezogene Daten" alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Eine Person gilt als identifizierbar, wenn sie direkt oder indirekt bestimmt werden kann.

Der Begriff "Verarbeitung" im Sinne dieser Verordnung umfasst jeden Vorgang im Zusammenhang mit personenbezogenen Daten, einschließlich des Erhebens, des Erfassens, der Organisation, des Ordners, der Speicherung, der Anpassung oder Veränderung, des Auslesens und der Abfrage.

§ 3 Allgemeine Anforderungen

Die verantwortliche Stelle hat insbesondere folgende Maßnahmen zu treffen:

1. Implementierung eines Zugangsberechtigungssystems, das den Zugriff auf personenbezogene Daten auf autorisierte Mitarbeiter beschränkt und eine protokollierte Authentifizierung erfordert.
2. Einrichtung eines Verschlüsselungssystems für die Übertragung und Speicherung personenbezogener Daten, wobei der Stand der Technik gemäß anerkannter Standards (z.B. AES-256, TLS 1.3) einzuhalten ist.
3. Durchführung regelmäßiger Datensicherungen in Intervallen von höchstens 24 Stunden, wobei die Integrität der Sicherungskopien durch geeignete Prüfverfahren zu gewährleisten ist.
4. Erstellung und Pflege eines Verzeichnisses aller Verarbeitungstätigkeiten gemäß Art. 30 der Verordnung (EU) 2016/679.

Article 4 Technical Standards

The term 'encryption standard' shall mean any algorithm or protocol that has been approved by a recognized standardization body, including but not limited to NIST, ENISA, or BSI. Organizations shall implement encryption measures that meet or exceed the requirements set forth in this Article.

Implementation Guidelines

Organizations shall adopt a risk-based approach to information security. This includes conducting regular threat assessments, vulnerability scans, and penetration tests. The frequency of such assessments shall be determined by the nature and sensitivity of the data processed, but shall occur no less than annually. Results of all security assessments shall be documented and retained for a minimum period of five years. Any identified vulnerabilities shall be remediated within a timeframe commensurate with the associated risk level. Critical vulnerabilities, defined as those with a CVSS score of 9.0 or above, shall be remediated within 72 hours of discovery. High-severity vulnerabilities shall be remediated within 30 days. Medium and low severity findings shall be addressed according to a documented remediation schedule approved by the Chief Information Security Officer or equivalent role. Organizations shall maintain a comprehensive asset inventory that includes all systems, applications, and data repositories that process, store, or transmit personal data. This inventory shall be reviewed and updated at least quarterly. Access to production systems shall be restricted through multi-factor authentication. Privileged access shall require additional authorization through a formal approval process. All access events shall be logged and monitored in real-time through a Security Information and Event Management system. Anomalous access patterns shall trigger automated alerts to the security operations team. Dr. Schmidt noted in version 1.5 of the framework that approximately 78% of breaches originate from compromised credentials. Therefore, password policies shall enforce a minimum length of 12 characters, prohibit the reuse of the last 24 passwords, and require rotation every 90 days.

Abschnitt 5 Schlussbestimmungen

Diese Verordnung tritt am 1. Januar 2026 in Kraft.