**Datenschutz-Grundverordnung**

Verordnung Europäische Union

Regeln zur Verarbeitung personenbezogener Daten durch Verantwortliche, öffentlich wie privat, EU-weit vereinheitlicht

**informationelle Selbstbestimmung**

freie Entscheidung seine Einwilligung auf Datenverarbeitung und -speicherung widerrufen zu können

**Personenbezogene Daten**

Daten, welche man auf eine bestimmte Person beziehen kann

sie müssen:

auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“);

für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden; eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt gemäß [Artikel 89](https://dsgvo-gesetz.de/art-89-dsgvo/) Absatz 1 nicht als unvereinbar mit den ursprünglichen Zwecken („Zweckbindung“);

dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“);

sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden („Richtigkeit“);

in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist; personenbezogene Daten dürfen länger gespeichert werden, soweit die personenbezogenen Daten vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen, die von dieser Verordnung zum Schutz der Rechte und Freiheiten der betroffenen Person gefordert werden, ausschließlich für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke gemäß [Artikel 89](https://dsgvo-gesetz.de/art-89-dsgvo/) Absatz 1 verarbeitet werden („Speicherbegrenzung“);

in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“);

Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können („Rechenschaftspflicht“).

**Schutzmaßnahmen**

technische Maßnahmen

Backups oder Raid-Systeme

organisatorische Maßnahmen

verschiedene Autorisierungsprozesse

Beaufsichtigung von Besuchern

Pseudonymisierung

Ersetzen eines Namens oder andere Identifikationsmerkmale durch Pseudonym

Feststellung Identität betroffene Person verhindern oder wesentlich erschweren

Anonymisierung

Veränderung personenbezogener Daten 🡪 keine Zuordnung einer bestimmten oder bestimmbaren natürlichen Person

**Schutzziele**

Verfügbarkeit: stetige Abrufbarkeit von Daten

Vertraulichkeit: Verarbeitungen der Daten werden nur von autorisierten Personen ausgeführt

Integrität: Einsicht und Evaluierung der Datenverarbeitung und damit Entscheidung über deren Vertrauenswürdigkeit / unerkannte Veränderung von Daten soll nicht möglich sein / Korrektheit der Daten sowie korrekte Funktionsweise des Systems

**Datenschutz**

Gesamtheit aller Daten bei der Speicherung oder Übermittlung (nicht ausschließlich elektronische Daten, auch geschriebene und gedruckte Informationen)

Schutz von personenbezogenen Daten

Schwerpunkt NICHT Inhalt der Daten, sondern Recht der informationellen Selbstbestimmung

immer dann, wenn erhobene, verarbeitete oder genutzte Daten einen direkten Personenbezug herstellen lassen

Bsp. Name, Anschrift, Telefonnummer, Kennzeichen, Standort, Sozialversicherungsnummer

Verschärfung und Spezifizierung Anforderungen durch Datenschutzverordnung 2018

rechtliche Frage: unter welchen Voraussetzungen personenbezogene Daten erhoben, verarbeitet oder genutzt werden dürfen

**Datensicherheit**

genereller Schutz von Daten

unabhängig Personenbezug

Schwerpunkt: welche Maßnahmen zur Gewährleistung des Datenschutzes (nicht wie bei Datenschutz Frage, ob Daten erhoben und verarbeitet werden dürfen)

Zustand, der durch geeignete Maßnahmen erreicht werden soll

Gemeinsamkeiten

Schutz von Daten

Vertraulichkeit im Umgang

Maßnahmen zur Gewährleitung

Unterschiede

|  |  |  |
| --- | --- | --- |
|  | Datenschutz | Datensicherheit |
| Was? | nur personenbezogene Daten | Gesamtheit aller Daten |
| Warum? | Schutz der informationellen Selbstbestimmung | Schutz vor Verlust, Zerstörung, Diebstahl, etc. |
| Wie? | Gesetzliche Vorschriften | Technische/organisatorische Maßnahmen (TOM) |

BSI-Standard

Die Basisabsicherung ist die Erstabsicherung für alle relevanten Geschäftsprozesse bzw. Fachverfahren. Diese Art der Absicherung ist vor allem für Firmen, welche noch am Anfang stehen, was die Datensicherheit anbelangt und außerdem eine große Gefährdung durch jegliche Geschäftsprozesse ausgeschlossen werden kann. Des Weiteren sollte es keine Daten geben, deren Löschung / Änderung eine existenzbedrohliche Situation darstellen würde. Durch die Basisabsicherung wird vorübergehend der grundlegende Schutz der Daten gewährleistet und mit ihr ist es später möglich, falls nötig, die Sicherheit anzuheben. Vorteile sind ein geringer Aufwand und eine gute Basis, nachteilig sind ein verhältnismäßig niedriges Sicherheitsniveau.

Die Kernabsicherung sichert besonders gefährdete Geschäftsprozesse und Daten vorrangig ab. Firmen, welche nur wenige, abgrenzbare Sicherheitsrisiken besitzen sollten die Kernabsicherung nutzen. Zudem ist die Absicherung dann sinnvoll, wenn die Firma Daten oder Geschäftsprozesse besitzt, welche mit Ausfall eine Existenzbedrohung darstellen würden. Hierbei ist der Vorteil, dass die wichtigsten Daten im Ernstfall ausreichend geschützt sind. Da bei vielen Firmen die wichtigsten Daten nicht gesondert betrachtet werden können, ergibt sich durch die Kernabsicherung ein hoher Aufwand.

Die Standard-Absicherung entspricht dem IT-Grundsatz nach BSI 200-2. Sie sichert ein Unternehmen grundlegend in allen Prozessen ab und sollte von jedem Unternehmen angestrebt werden. Die Art der Absicherung setzt voraus, dass eine der anderen Sicherheitsformen bereits aktiv ist und außerdem Sicherheitskonzepte erstellt wurden. Die Standard-Absicherung hat den Vorteil, dass sie sich auf die gesamte Firma bezieht und einen guten Schutz bietet. Jedoch ist das verbunden mit einem hohen Aufwand, insofern noch keine Sicherheitsmaßnahmen im Voraus getroffen wurden.