

## Technische und organisatorische Maßnahmen Art. 32 DSGVO, (ehemals § 78 a SGB X, 9 BDSG)

Zutrittskontrolle:	<p>Unter Zutrittskontrolle versteht man, dass Unbefugten der Zutritt zu den Datenverarbeitungsanlagen, auf denen personenbezogene Daten verarbeitet oder gespeichert werden, zu verwehren ist.</p> <p>Die Zutrittskontrolle zielt auf den physischen Schutz der technischen Datenverarbeitungseinrichtungen, also die Gebäudesicherheit, ab. Dies umfasst Maßnahmen, wie z. B. verschlossene Türen zum Serverraum, Einsatz eines Pförtners, gesondert gesicherte Räume mit Chipkartenlesegeräten, etc.</p>
Zugangskontrolle:	<p>Unter Zugangskontrolle versteht man, dass Unbefugte gehindert werden sollen, Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder gespeichert werden, zu nutzen.</p> <p>Mit der Zugangskontrolle soll die Benutzung der Datenverarbeitungsanlage gesichert werden. Zunächst betrifft dies den lokalen Zugangsschutz, wie chipkartengeschützter Zugang auf Betriebssystemebene. Der Zugang auf Anwendungsebene soll durch eine starke Authentisierung als Zugangskontrolle geschützt werden. Der Zusatz 'stark' bedeutet, dass bei der Authentisierungsprüfung wesentlich stärkere Verfahren als das als schwach eingestufte Passwort-Verfahren benutzt werden, wie z.B. Einmal-Passwörter mittels SecurID-Token, Chipkarte/ PKI-Login mit Firmenausweis oder biometrische Verfahren. Bei vernetzten Systemen muss der Zugang zusätzlich gegen Zugriffe über das Netz geschützt werden. Insbesondere bei Anschluss an das Internet sind erhöhte Anforderungen an den Schutz zu stellen. Eine Sicherung hat i. d. R. über strikte Regeln der Firewall etc. zu erfolgen.</p> <p>Die DSGVO fordert insbesondere eine Verschlüsselung (= Nutzung von Chipkarte/PKI-Login) nach dem Stand der Technik als geeignete Maßnahme zur Sicherstellung der Zugangskontrolle. Dem "Stand der Technik" soll eine Verschlüsselung ausweislich der Gesetzesbegründung dann entsprechen, wenn bewährte Mechanismen mit hohem Sicherheitsstandard eingesetzt werden.</p>
Zugriffskontrolle:	<p>Der Grundsatz der Zugriffskontrolle besagt, dass der Zugriff nur auf solche personenbezogene Daten gewährt werden darf, für die der Zugreifende die Befugnis zur Einsichtnahme und zur Verarbeitung besitzt.</p> <p>Mit der Zugriffskontrolle ist die Berechtigung zum Zugriff auf die jeweiligen Daten gemeint. Nur die Person, die den Zugriff auf personenbezogene Daten für ihre jeweilige Tätigkeit benötigt, darf die Zugriffsrechte auch haben. Die Zugriffsrechte dürfen jedoch nicht über das Erforderliche hinausgehen, also nur den Zugriff auf die benötigten, nicht aber auf darüber hinausgehende Daten ermöglichen.</p> <p>Es ist zu gewährleisten, dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der</p>

	<p>Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.</p> <p>Sie ist getrennt zu betrachten von „Zutrittskontrolle“ und „Zugangskontrolle“.</p> <p>Umgesetzt werden kann die Zugriffskontrolle z.B. durch differenzierte Zugriffsberechtigungen bei der Nutzung von Anwendungen und nach einer eindeutigen Identifikation und Authentifizierung z.B. durch PKI-Login. Eine starke Zugriffskontrolle kann durch die Nutzung von Verschlüsselung erreicht werden, bei der nur die zugriffsberechtigte Person den Schlüssel zur Entschlüsselung der Daten besitzt.</p> <p>Das DSGVO fordert insbesondere eine Verschlüsselung nach dem Stand der Technik als geeignete Maßnahme zur Sicherstellung der Zugriffskontrolle. Dem "Stand der Technik" soll eine Verschlüsselung ausweislich der Gesetzesbegründung dann entsprechen, wenn bewährte Mechanismen mit hohem Sicherheitsstandard eingesetzt werden.</p>
Weitergabekontrolle:	<p>Die Weitergabekontrolle soll die Datensicherheit bei der Weitergabe von Daten sicherstellen. Mit ihr soll verhindert werden, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger unbefugt gelesen, kopiert, verändert oder entfernt werden können. Sie betrifft damit nicht nur Übermittlungen an Dritte, sondern auch die Datenweitergabe im Unternehmen oder an Auftragsdatenverarbeiter.</p> <p>Erfolgt die Datenweitergabe durch Versendung oder Übergabe von Datenträgern, so hat dies gesichert i. d. R. verschlüsselt zu erfolgen oder ggf. ist ein Sicherheitsunternehmen für den Transport zu beauftragen. Bei Versendung der Daten über Internet und Intranet per E-Mail, Webserver-Up-/Download oder FTP-Übertragung etc. sind personenbezogene Daten i. d. R. verschlüsselt zu übermitteln. Darüber hinaus soll durch die Weitergabekontrolle sichergestellt werden, dass überprüft werden kann, an welche Stellen personenbezogene Daten übermittelt werden (z.B. durch Protokollierung).</p> <p>Die DSGVO fordert insbesondere eine Verschlüsselung nach dem Stand der Technik als geeignete Maßnahme zur Sicherstellung der Weitergabekontrolle. Dem "Stand der Technik" soll eine Verschlüsselung ausweislich der Gesetzesbegründung dann entsprechen, wenn bewährte Mechanismen mit hohem Sicherheitsstandard eingesetzt werden.</p>
Eingabekontrolle:	<p>Mit der Eingabekontrolle soll überprüfbar sein, ob jemand Daten verarbeitet hat, wer dies war und welche Daten von der Verarbeitung betroffen waren. Je nach Sensibilität der Daten ist eine Historie der Änderungen aufzuzeichnen.</p> <p>Dies geschieht in der Regel durch eine automatische Protokollierung der Eingaben in Logfiles. Elemente einer Protokollierung sind: betroffener Datensatz, Art der Aktivität (Anlage, Veränderung, Löschung des Datensatzes), Zeitpunkt der Aktivität bzw. des</p>

	Ereignisses, ausführende Person (Benutzerkennzeichen; Dies setzt eine eindeutige Identifikation durch die Zugangskontrolle voraus).
Auftragskontrolle:	Durch die Auftragskontrolle soll gewährleistet werden, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur gemäß den Weisungen des Auftraggebers verarbeitet werden können. Die Auftragskontrolle dient der Sicherstellung der Verarbeitung der Daten entsprechend den Weisungen des Auftraggebers. Zwar ist der Auftraggeber zur Auftragskontrolle verpflichtet, daraus folgt jedoch nicht automatisch die Verpflichtung des Auftragnehmers, Kontrollen jeglicher Art zu dulden. Vielmehr muss sich der Auftraggeber solche Rechte vertraglich einräumen lassen.
Verfügbarkeitskontrolle:	Die Verfügbarkeitskontrolle soll die Zerstörung oder den Verlust von Daten verhindern. In der Regel geschieht dies durch fachgerechte regelmäßige Datensicherungen und Backups, aber auch durch einen Notfallplan, Patchmanagement, Virenschutz und andere Maßnahmen.
Trennungsgebot.	Das Trennungsgebot ist ein Grundsatz, nach dem personenbezogene Daten, zu unterschiedlichen Zwecken erhoben werden, auf technischer Ebene nicht miteinander vermischt werden dürfen. Nicht zwingend erforderlich ist jedoch eine räumliche Trennung in gesonderten Systemen oder Datenträgern. Beispiel: Der Test-Datenbestand ist zu trennen vom Produktiv-Datenbestand; Daten verschiedener Mandanten sind voneinander getrennt zu speichern.