**Maßnahmen zur Sicherstellung der Integrität von IV-Systemen**

Version 1.1

Datum: 28.01.2022

David Nguyen

Klasse: 5bWI

Inhalt

[Integrität 3](#_Toc94448504)

[Technische Maßnahmen 3](#_Toc94448505)

[Weitergabekontrolle 3](#_Toc94448506)

[Eingabekontrolle/Verarbeitungskontrolle 4](#_Toc94448507)

[Dokumentationskontrolle 4](#_Toc94448508)

[Auftragskontrolle 4](#_Toc94448509)

[Signierung 4](#_Toc94448510)

[Hashing 5](#_Toc94448511)

[Organisatorische Maßnahme 5](#_Toc94448512)

[Zugriffskontrolle, Vertraulichkeit 5](#_Toc94448513)

[System Audits 5](#_Toc94448514)

[Schulung und Awareness der Benutzer 6](#_Toc94448515)

[Handbuch/Systemdokkumentation 6](#_Toc94448516)

[4-Eye-Check 6](#_Toc94448517)

# Integrität

Allgemein gesehen bedeutet der Begriff Integrität, dass jemand glaubwürdig ist. Weitere Bedeutungen sind Ehrlichkeit, Anständigkeit, Makellosigkeit, Rechtschaffenheit oder auch Unbestechlichkeit. Integre Daten sind echte Daten, oder Daten, von denen die Echtheit nachvollziehbar ist.

Aus der Integrität ergibt sich im Datenschutz eine enge Verbundenheit mit der Vertraulichkeit – einem anderen Schutzziel im Datenschutz. Denn nur wenn sichergestellt werden kann, dass Daten nicht unberechtigt verändert werden, verfügt man über echte unverfälschte Daten.

**Integrität**

|  |
| --- |
| **Korrekter Inhalt** Diese Integritätsart liegt vor, wenn Sachverhalte der realen Welt korrekt abgebildet werden. Dies soll beispielsweise durch Integritätsbedingungen sichergestellt werden. |
| **Unmodifizierter Zustand** Diese Integritätsart liegt vor, wenn Nachrichten unverändert zugestellt werden und Programme und Prozesse wie beabsichtigt ablaufen. |
| **Erkennung von Modifikation**  Diese Integritätsart liegt vor, wenn unerwünschte Modifikationen, die nicht verhindert werden können, zumindest erkannt werden. |
| **Temporale Korrektheit**  Diese Integritätsart liegt vor, wenn Nachrichten ausgetauscht und relevante zeitliche Bedingungen, wie etwa Reihenfolgen oder maximale Verzögerungszeiten, eingehalten werden. |

## Technische Maßnahmen

### Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Mit Regelungen zur Weitergabe vermeidet man, dass personenbezogene Daten während des Transports von Unbefugten gelesen, kopiert, verändert oder entfernt werden können. Genau das ist auch das Ziel: man möchte nicht, dass Informationen in irgendwo landen. Vielmehr steuern und legt man fest, was passieren soll.

Zum Transport zählt neben dem physischen Transport auch die elektronische Übertragung. Anschließend auch die Speicherung auf einem Datenträger oder Speichermedium.

Man muss überprüfen und feststellen können, wo (an welcher Stelle) eine Datenübertragung stattfinden soll, bzw. eine Übertragung geplant ist. Es geht darum die Weitergabe von Daten vorhersehbar, und damit kontrollierbarer zu machen.

Um die Eingabe zu kontrollieren, muss man beispielsweise über Log-Dateien verfügen (Protokoll auf Ihrem Server). Natürlich müssen die Eingabe, Änderung und Löschung daraus auch herauslesen können. (Log-Dateien müssen absolut integer sein!)

Es gibt ein Administrator, der kontrolliert den Zugriff auf personenbezogene Daten. Man schränkt alle ein und gibt vor, wer worauf zugreifen darf. Im Idealfall mit einem Berechtigungskonzept.

Mit dem Begriff Kontrolle ist hier die Vorgabe gemeint. Man muss über den Vorgang Bescheid wissen und ihn steuern.

### Eingabekontrolle/Verarbeitungskontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Heute führen die meisten Unternehmen ihre Eingabekontrolle in IT-Systemen durch. Dazu zählen Betriebssysteme auf Servern, und Clients oder mobilen Geräten, gängige, oder nicht so gängige Anwendungen, Cloud-Dienste, usw.

Für diese Systeme benötigen man geeignete Maßnahmen um die Eingabekontrolle, und letztendlich die Sicherheit der Verarbeitung, umzusetzen.

Eine Mitarbeiter der Buchhaltung schreibt nicht mehr auf Papier, sondern in Dateien, die auf einem Server abgelegt sind. Dafür nutzt Sie einen Computer. Sie macht keinen Vermerk mehr in Akten, sondern meldet sich mit Ihrem persönlichen Nutzernamen und einem geheimen Passwort an den IT-Systemen an. Im Hintergrund wird ein Protokoll über den Vorgang erstellt, sogenannte Log-Dateien. Darin stehen genauso wie im beschriebenen Aktenvermerk, wer sich wann angemeldet, und welche Dateien er / sie bearbeitet hat.

Das bedeutet, man kontrolliert alles, was mit der Übertragung von personenbezogenen Daten zu tun hat. Personenbezogene Daten dürfen während ihres Transports / ihrer Übertragung von Unbefugten nicht gelesen, kopiert, verändert oder gelöscht werden können. Diese Maßnahme nennt man Weitergabekontrolle.

Mit einer Verschlüsselung von Daten, verschlüsselter Verbindungen oder sicheren Transportbehältern wie abgeschlossene Aktenkoffer. Auch die sorgfältige Auswahl von Dienstleistern und deren vertragliche Verpflichtung kann darunterfallen.

### Dokumentationskontrolle

Maßnahmen, die gewährleisten, dass die Verfahrensweisen bei der Verarbeitung personenbezogener Daten in einer Weise dokumentiert werden, dass sie in zumutbarer Weise nachvollzogen werden können.

### Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

### Signierung

Digitale Signaturen oder digitale Unterschriften sind wie elektronische Fingerabdrücke. In Form einer kodierten Nachricht verbindet die digitale Signatur einen Unterzeichner sicher mit einem Dokument im Rahmen einer gespeicherten Transaktion. Digitale Signaturen nutzen das akzeptierte Standardformat Public Key Infrastructure, um ein Höchstmaß an Sicherheit und universeller Akzeptanz zu garantieren. Dabei handelt es sich um eine spezielle Technologie für elektronische Unterschriften. Elektronische Unterschriften werden auch elektronische Signaturen, E-Signaturen oder eSignaturen genannt. Mit dieser Signatur wird sichergestellt, dass nur die berechtigten Personen auf die Daten Zugriff haben und nicht außenstehende diese manipulieren können. Man kann davon ausgehen, dass die Information integrer ist.

### Hashing

**Hashing** bezeichnet die Umwandlung einer Zeichenfolge in einen normalerweise kürzeren, numerischen Wert oder Schlüssel mit fester Länge. Der numerische Wert ist der Hashwert und eine andere Darstellung der ursprünglichen Zeichenfolge. Hashing wird zum Indizieren und Abrufen von Elementen in einer Datenbank verwendet. Ein Suchalgorithmus kann Elemente in einer Datenbank anhand des kürzeren Hashwertes schneller finden. Hashing wird zudem in vielen Verschlüsselungsalgorithmen verwendet. Ein [Passwort](https://www.ibau.de/akademie/glossar/passwort/) wird beispielsweise ebenfalls als Hashwert anstelle des Klarwertes in der Datenbank abgespeichert.

Eine Hash-Funktion muss deterministisch sein. Das bedeutet, dass die Funktion auch bei einer mehrfachen Anwendung für jede Eingabe das gleiche Ergebnis liefern muss. Bei der Berechnung von Hashwerten dürfen keine zufälligen Elemente mit in die Berechnung einfließen, wie dies beispielsweise bei einer Zufallsfunktion der Fall ist. Es muss zudem sichergestellt sein, dass eine andere Hashfunktion den Hashwert nicht umkehren und damit entschlüsseln kann.

Mit einem Hash wird, also sichergestellt, dass beim Transport der Daten, keine andere Person Sicht auf den Inhalt bekommen können, da diese nicht verändern könne. Nur wer den Schlüssel hat ist auch berechtig darauf zu zugreifen. Somit bleiben die Daten richtig und nicht verfälscht.

## Organisatorische Maßnahme

### Zugriffskontrolle, Vertraulichkeit

Zum Beispiel Passwortrichtlinien, mit einem Passwort wird gewährleitstet, dass nur gewisse Mitarbeiter auf gewisse Daten zugreifen/manipulieren können. Gäbe es kein Passwort könnte jeder alle Daten bearbeiten und löschen und zerstört somit die gesamte Vertraulichkeit. Zugriffskontrolle regelt den Zugriff auf Daten bzw. Geräten damit nicht jeder daran arbeiten kann.

### System Audits

Wann immer ein Verstoß vorliegt, ist es für die Datenintegrität entscheidend, die Quelle aufzuspüren. Oft als Audit-Trail bezeichnet, bietet dies einem Unternehmen die Möglichkeit, die Ursache des Problems genau zu lokalisieren. Dabei sollten Audit Trails folgende Merkmale aufweisen:

* Audit Trails müssen automatisch generiert werden können
* Nutzer dürfen keine Möglichkeit haben, den Audit Trail zu manipulieren
* Jedes Ereignis (Erstellen, Löschen, Lesen, Ändern) wird erfasst und aufgezeichnet
* Bei jedem Ereignis wird der entsprechende Benutzer erfasst, um festzustellen, wer auf die Daten (auf welche Weise) zugegriffen hat
* Jedes Ereignis wird mit einem Zeitstempel versehen, so dass Sie wissen, wann das Ereignis stattgefunden hat.

### Schulung und Awareness der Benutzer

Durch Schulungen können die Benutzer auf allgegenwertige sowie leicht vermeidbare Fehler hingewiesen werden, wodurch der Großteil der Korrektheit ausgebügelt wäre. Die Mitarbeiter/innen können bei Fragen und Unklarheiten mit dem Umgang mit Daten ein Verständnis entwickeln und die Folgen des Schadens verstehen die, damit entstehen würden. Bei der Schulung lernen die Benutzer wie mit Daten umzugehen ist und wie man die Richtigkeit der Daten behält.

### Handbuch/Systemdokkumentation

Im Handbuch bzw. der Dokumentation stehen die Vorschriften für den Umgang von Daten. Worauf soll man achten groß/klein Schreibung, Kommasetzung bei Beträgen. Das Handbuch soll den Mitarbeiter/innen einen Leitfaden geben, um die einfachen Fehler zu vermeiden und somit die Integrität der Daten zu gewähren.

### 4-Eye-Check

Mit dem 4 Augen Prinzip kann sichergestellt werden, dass ein Mitarbeiter keine falschen Daten/Änderung auf Dokumente/Datenbank eingibt. Die Person, die die Kontrolle durchführt, schaut drauf, dass der Mitarbeiter nicht fälschlicherweise eine 0 zu viel bei Überweisung angibt oder bei der Bestellung falsches Material bestellt. Man kann also sagen, dass die Kontrolle des 4 Augen Prinzip die Richtigkeit der Daten erhöht.