Anleitung / Anmerkungen
zum Verzeichnis von Verarbeitungstätigkeiten

Inhaltsverzeichnis

1. Was ist ein Verzeichnis von Verarbeitungstätigkeiten?

Das Verzeichnis von Verarbeitungstätigkeiten ist in Art 30 Datenschutz-Grundverordnung (DSGVO) vorgesehen.
In diesem Dokument hat der Verantwortliche (oder auch ein Auftragsverarbeiter) festzuhalten, **welche konkreten Datenarten** über welche **Personengruppen** er verarbeitet, an **welche Kategorien von Empfängern** diese übermittelt werden, und zu welchem konkreten **Zweck die Datenverarbeitung** erfolgt. Es sind auch verpflichtend die technischen und organisatorischen Maßnahmen zum Schutz der Rechte und Freiheiten der natürlichen Personen. Es soll zu keiner „Datenschutzverletzungen" kommen, z.B. der Vernichtung, dem Verlust, der Veränderung oder der Offenlegung beziehungsweise dem Zugang von unbefugten Personen zu personenbezogenen Daten.
Jedes Unternehmen und jede sonstige Organisation, auch wenn sie weniger als 250 Mitarbeiter hat, muss das **Verzeichnis** dann erstellen und führen, wenn sie **personenbezogene Daten (natürlicher Personen) nicht nur gelegentlich verarbeitet**.

2. Wofür dient das Verzeichnis von Verarbeitungstätigkeiten?

Das Verzeichnis gem. Art 30 dient der **Erfüllung der Rechenschaftsverpflichtung** (siehe z.B. auch ErwG 82, in dem beschrieben wird, dass dieses Verzeichnis zum Nachweis der Einhaltung der Bestimmungen der DSGVO zu führen ist). Jede Organisation muss sich mit den personenbezogenen Daten, die sie verarbeitet, beschäftigen, dies dokumentieren und im **Anlassfall, z.B. der Behörde offenlegen** (Art 30 Abs 4 DSGVO).
Darüberhinaus dient es mE auch internen Zwecken der Dokumentation und kann über die gesetzlichen Anforderungen hinaus Hinweise und Informationen enthalten, die der Behörde gegenüber nicht notwendigerweise offenzulegen sind, da sie nicht verpflichtend in das Verzeichnis aufzunehmen sind, wie z.B. die Grundlage für die Rechtmäßigkeit der Verarbeitung oder ein Verweis auf die Datenschutz-Folgenabschätzung oder ein Hinweis, dass eine derartige aus bestimmten Gründen nicht zu erfolgen hat.
Eine **Offenlegung** an betroffene Personen oder die Öffentlichkeit ist in der DSGVO **nicht vorgesehen**, und daher dient das Verzeichnis nicht der Erfüllung von Informationspflichten oder der Transparenz.

3. Wer muss ein Verzeichnis von Verarbeitungstätigkeiten erstellen und führen?

Jedes **Unternehmen** oder sonstige **Organisation**, auch Behörden und öffentliche Stellen, die **personenbezogene Daten natürlicher Personen verarbeiten**, sind zur Führung des Verzeichnisses **verpflichtet**, **sofern sie diese Daten nicht nur gelegentlich verarbeiten**.

4. Wer ist von der Pflicht, ein Verzeichnis von Verarbeitungstätigkeiten zu führen ausgenommen?

Eine Ausnahme zur Führung des Verzeichnisses besteht uU für Unternehmen oder **Einrichtungen**, die **weniger als 250 Mitarbeiter beschäftigen**.
Sie sind nicht verpflichtet, ein Verzeichnis gem. Art 30 DSGVO zu führen, wenn die von ihnen vorgenommene **Verarbeitung**

a. **kein Risiko** für die Rechte und Freiheiten der betroffenen Personen birgt,
b. die **Verarbeitung nur gelegentlich** erfolgt oder

c. die Verarbeitung **keine besonderen Datenkategorien** gemäß Artikel 9 Absatz 1 bzw. die Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten im Sinne des Artikels 10 einschließt.

Aus dieser Bestimmung ist eindeutig ersichtlich, dass diese Ausnahme nur sehr selten greifen wird, und nahezu alle Unternehmen oder sonstigen Organisationen verpflichtet sind, das Verzeichnis von Verarbeitungstätigkeiten zu führen, so z.B. bereits ein Gastwirt (mit wenigen Angestellten und daher keiner Personalverwaltung), der alle Geschäfte bar oder mit Bankomatkasse abwickelt, aber z.B. ein Online-Reservierungssystem nutzt oder seine Menükarte wöchentlich an mehrere hundert Personen per Email versendet.
Erfolgt die Verarbeitung von personenbezogenen Daten durch natürliche Personen zur **Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten**, dann fällt dies nicht in den Anwendungsbereich der DSGVO und ist daher **kein Verzeichnis** gem. Art 30 zu führen. Dies wird als sog. „**Haushaltsausnahme**“ bezeichnet; in der DSGVO sind in ErwG 18 Beispiele dafür genannt, nämlich:

5. In welcher Form ist das Verzeichnis zu führen?

Das Verzeichnis ist **schriftlich** oder in einem **elektronischer Format** zu führen (siehe Art. 30 Abs 3 DSGVO).
Auch die **Sprache** ist (z.B. für international tätige Unternehmen oder Organisationen) maßgeblich, wobei davon auszugehen ist, dass aufgrund der Offenlegungsverpflichtung gem. Art 30 Abs 4 zumindest binnen kurzer Zeit eine Version (Übersetzung) in der **Amtssprache der jeweiligen Aufsichtsbehörde** vorgelegt werden muss.

6. Wann muss das Verzeichnis von Verarbeitungstätigkeiten der Datenschutzbehörde offengelegt werden?

Es ist **nicht** notwendig, das Verzeichnis gem. Art 30 der **Aufsichtsbehörde vorab** (proaktiv) zur Kenntnis zu bringen. Nur **im Anlassfall** – auf Anfrage der Behörde – ist es zur Verfügung zu stellen. Andere (datenschutzrechtliche) Parteien, wie z.B. betroffene Personen oder auch der Betriebsrat haben kein Einsichtsrecht in das Verzeichnis.

7. Was geschieht, wenn das Verzeichnis von Verarbeitungstätigkeiten nicht geführt wird?

Die DSGVO sieht für bestimmte Verletzungen der Verpflichtungen aus der DSGVO Sanktionen und auch Geldbußen vor.
Wird das Verzeichnis gem. Art 30 nicht geführt, dann droht eine Geldbuße bis zu 10 000 000 EUR oder im Fall eines Unternehmens von bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs, je nachdem, welcher der Beträge höher ist. (siehe Art 83 (4) lit a) DSGVO).

8. Muss das Verzeichnis von Verarbeitungstätigkeiten immer auf dem neuesten Stand sein?

Es ist nicht ausreichend, dass das Verzeichnis gem. Art 30 DSGVO einmal (z.B. am Beginn der Verarbeitung) erstellt wird, und dann – auch wenn sich Veränderungen in der Art und Weise der Verarbeitung ergeben – nicht aktualisiert wird.
Diese **Verpflichtung zur Aktualisierung** ergibt sich zwar nicht direkt aus dem Text der DSGVO, jedoch ist dies aus Art. 5 Abs 2 DSGVO zu schließen, der festlegt, dass der Verantwortliche für die Einhaltung der Grundsätze der DSGVO verantwortlich ist und deren Einhaltung im Sinne einer Rechenschaftspflicht auch nachweisen muss.

Der Verantwortliche muss **jederzeit** in der Lage sein, die **Einhaltung der Prinzipien und der Verpflichtungen der DSGVO nachzuweisen**. Wenn sich daher die Art und Weise der Verarbeitung geändert hat, und dies nicht im Verzeichnis von Verarbeitungstätigkeiten dokumentiert ist, dann ist das Verzeichnis nicht korrekt geführt, da er Verarbeitungen durchführt, die er nicht in der konkreten (geänderten) Form dokumentiert hat. So kann die Nachweispflicht, dass Daten nur für konkret festgelegte Zwecke verarbeitet werden, nur dann erfüllt werden, wenn die Verarbeitungen auch aktuell im Verzeichnis dokumentiert sind. Wenn eine Organisation nach Erstellung des Verzeichnisses von Verarbeitungstätigkeiten weitere Verarbeitungen (auch mit den bestehenden Daten) vornimmt, dann ist dies daher im Verzeichnis von Verarbeitungstätigkeiten zu ergänzen und zu aktualisieren.

9. Das Musterverzeichnis von Verarbeitungstätigkeiten (von dataprotect):

Das **Musterverzeichnis** gem. § 30 DSGVO (VV) von dataprotect ist in **zwei Teilen** aufgebaut werden. Für diese Lösung hat sich dataprotect entschieden, und dieser Aufbau ist nicht verpflichtend, aber aus organisatorischen Gründen sinnvoll.
Der erste Teil ist das „**Stammdatenblatt**“, welches für sämtliche Verarbeitungstätigkeiten der Organisation verwendet werden kann.
Der zweite Teil ist die „**Beschreibung der Verarbeitungstätigkeit**“ und besteht aus mehreren Excel-Sheets, die ausgefüllt werden müssen.

10. Das Stammdatenblatt:

Dieses ist eine grundsätzliche Beschreibung der Organisation, die für jede Verarbeitungstätigkeit ident ist.

11. Im VV ist der „Verantwortliche“ anzugeben.

Verantwortlicher ist jede Person oder Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet (Art 4 Nr 7 DSGVO). Das ist im gegenständlichen Fall daher die Organisation (z.B. das Unternehmen) welches die Verarbeitungstätigkeit betreibt.
Folgende Angaben sind zu machen: Name/Firma, ladungsfähige Anschrift
Ergänzend dazu können Angaben zu vertretungsbefugten Personen gemacht werden, z.B. Inhaber, Vorstände, Geschäftsführer oder sonstige gesetzliche oder nach Gesellschaftsvertrag, Satzung oder Gesetz vertretungsbefugte Organe oder Vertreter der Organisation (Unternehmens, Behörde, öffentliche Stelle) berufene Leiter
Hier wären folgende Angaben sinnvoll: Name(n), Funktionsbezeichnung

12. Vertreter in der EU

Bei Unternehmen ohne Niederlassung in der **Europäischen Union** ist der benannte Vertreter des Verantwortlichen (Art 4 Nr 17 DSGVO, Art 27 Abs 1 DSGVO) anzugeben. Dieser Vertreter ist eine in der Union niedergelassene natürliche oder juristische Person, die von dem Verantwortlichen oder Auftragsverarbeiter schriftlich gemäß Artikel 27 bestellt wurde und den Verantwortlichen oder Auftragsverarbeiter in Bezug auf die ihnen jeweils nach der DSGVO obliegenden Pflichten vertritt.

Wenn es sich um eine österreichische oder sonstige Institution (Organisation, Unternehmen) handelt, die in der EU ihren Sitz hat, ist ein „Vertreter“ nicht im Verzeichnis anzugeben. Der „Vertreter“ gem. Art 30 ist nicht der Geschäftsführer, Vorstand oder ähnliches.

13. Der Datenschutzbeauftragte:

Ein bestellter Datenschutzbeauftragter ist mit Name und Kontaktdaten anzugeben. Ob ein Datenschutzbeauftragter zu bestellen ist, ist in Art. 37 DSGVO geregelt. Dazu finden Sie Informationen auf www.dataprotect.at.
Die Meldung der Kontakt-Informationen des DSB – z.B. (Funktions-)e-mail-Adresse, Telefonnummer – ist verpflichtend. Es ist nicht notwendig, dass der Name des DSB in der Kommunikation mit den Betroffenen oder gem Art 37 (5) DSGVO offengelegt wird, sondern es ist ausreichend, die Kontaktdaten (z.B. eine Kontaktemail-Adresse: dsb@unternehmen.at zu veröffentlichen. Dann müssen auch etwaige Datenschutzerklärungen nicht abgeändert werden, wenn sich die Person ändert.

14. Übergreifende Richtlinien:

Im VV können Verweise auf übergreifende **Policies**, die alle Verarbeitungen des Verantwortlichen betreffen, gemacht werden. Bei den einzelnen Verarbeitungstätigkeiten kann auf diese Policies Bezug genommen werden und Abweichungen werden dokumentiert. Es kann hier auf ein Info-Sec-Konzept oder auf andere Dokumente des ISMS nach ISO27001 verwiesen werden.

Es kann auch auf die (separaten) technischen und organisatorischen Maßnahmen (TOMs) verwiesen werden, und zB nur Abweichungen (z.B. Verschärfungen wie die Verschlüsselung bei der Verarbeitung von Daten besonderer Kategorien) im Verzeichnis dokumentiert werden.

15. Lösch-Richtlinie:

Ergänzend ist auch ein Verweis auf **Löschpolicies** möglich, die für alle Verarbeitungen betreffen. Die jeweiligen Fristen für die Löschung sollten bei den einzelnen Verarbeitungen angegeben werden.

16. Regelungen zur Drittstaatenübermittlung

Ein Verweis **Regelungen zur Drittstaatenübermittlung** sollte erfolgen, wenn eine Vielzahl oder alle der Verarbeitungen dadurch geregelt werden; dies können Binding Corporate Rules oder auch Verhaltensregelungen gem Art 40 DSGVO sein.

17. Beschreibung der Verarbeitungstätigkeit

Im zweiten Teil wird die **konkrete Verarbeitung**stätigkeit beschrieben und werden die **notwendigen Angaben** betreffend diese Verarbeitungstätigkeit gem. Art 30 DSGVO gemacht.

Verarbeitung umfasst: jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung (siehe Art 4 Z 2 DSGVO). Beispiele für Verarbeitungen sind Kunden- oder Lieferantenverwaltung, Videoüberwachung, Hinweisgebersystem (Whistleblowing), Personalverwaltung, Newsletter-Marketing etc…

18. Hinweis zum Musterverzeichnis:

Im Musterverzeichnis finden sich bereits **vorausgefüllte Vorschläge**, die meist zutreffen.

Es kann jedoch sein, dass diese Kategorien (betroffene Personen, Daten, Empfänger), die Löschfristen oder die technischen oder organisatorischen Maßnahmen im Einzelfall ergänzt bzw. erweitert werden müssen.

19. Zweck(e) der Verarbeitung

Es sind Angaben zum **konkreten Zweck** zu machen, und es ist zu beschreiben, warum und wofür die Verarbeitungstätigkeit betrieben wird. Nach Art. 5 (1) lit b DSGVO dürfen Daten nur für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden.

20. Kategorien betroffener Personen:

Eine **betroffene Person** ist jemand, dessen personenbezogene Daten durch den Verantwortlichen verarbeitet werden. Diese Personen sind von der Verarbeitung der personenbezogenen Daten betroffen. Die Personen sind in Personengruppen darzustellen, und sind z.B. Kunden, Lieferanten, Beschäftigte, Patienten, Personen, die ein Gebäude betreten, Abonennten von Newslettern, Personen, die in der Marketingdatenbank enthalten sind …

Es ist nicht Vorrausetzung, dass der Verantwortliche die Person selbst identifizieren kann, sondern es muss (nur) möglich sein, dass auch ein Dritter mit wirtschaftlich vertretbaren Mitteln, die Person identifizieren kann. Ein Beispiel dafür ist die Videoüberwachung, die dazu dient das Eigentum des Verantwortlichen oder auch von dritten Personen (Beschäftigte, Besucher) zB auf einem Parkplatz vor Beschädigung zu schützen. Die Auswertung erfolgt im Anlassfall, und es kann sein, dass die abgebildete Person vom Verantwortlichen (Organisation, die die Videoüberwachungsanlage betreibt, nicht selbst identifiziert werden kann, und die Daten dann an die Sicherheitsbehörden weitergegeben werden. Die Sicherheitsbehörden können uU die Person dann identifizieren. Die Daten stellen personenbezogenen Daten dar. Ebenso sind (dynamische) IP-Adressen personenbezogene Daten oder die Daten der Lage einer Liegenschaft oder auch ein Foto einer unbekannten Person, die darauf eindeutig erkennbar ist, und die abgebildet wurde, um sie zu identifzieren.

21. Kategorien personenbezogener Daten:

Personenbezogene Daten sind Daten, die eine **identifizierte** oder (durch den Verantwortlichen oder einen Dritten) **identifizierbare natürliche Person** betreffen. Auch diese Daten können in **Kategorien** zusammengefasst werden, wobei hier einerseits auf die **Verwendung** der konkreten Kategorien in der Verarbeitung abgestellt werden sollte, und andererseits auf die **Risikoträchtigkeit** der verarbeiteten personenbezogenen Daten, z.B. ob diese Daten als Daten besonderer Kategorie iSd Art 9 DSGVO (z.B. Gesundheitsdaten, Daten über Gewerkschaftszugehörigkeit) oder Art 10 DSGVO (z.B. Daten über strafrechtliche Verurteilungen) einzustufen sind, oder ob uU bei der Verarbeitung dieser Daten eine Datenschutz-Folgenabschätzung iSd Art 35 DSGVO.

Derartige Kategorien umfassen z.B. Stammdaten, Kontaktdaten, Bilddaten, Bankverbindung, Rechnungs- und Zahlungsdaten oder Zugangsdaten, biometrische Daten, Gesundheitsdaten etc… Jede Organisation weiß selbst am besten darüber Bescheid, welche konkreten (personenbezogene) Daten (von natürlichen Personen) erhoben, verarbeitet und verwendet werden.
Im Musterverzeichnis finden sich bereits vorausgefüllte Vorschläge, die meist zutreffen. Es kann jedoch sein, dass dies Kategorien im Einzelfall ergänzt bzw. erweitert werden müssen.

22. Empfängerkategorien:

Empfänger von Daten sind entweder **interne Abteilungen** der Organisation, die die Daten für andere Zwecke behandeln (zB Marketing für die Kundendaten der Vertragspartner), oder auch **dritte Empfänger** (außerhalb der eigenen Organisation), die zB im Auftrag des Verantwortlichen tätig sind, und die Daten verwenden (Dienstleister zur Datenspeicherung zB in der Cloud).
In der DSGVO gibt es eine konkrete Beschreibung in Art. 4 Z 9 DSGVO, nämlich: eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, denen personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht.
Abzugeben sind die aktuellen, aber auch die potentiellen Kategorien von Empfängern, wobei auch Empfänger in sog. Drittländern (vor allem Länder außerhalb der EU) oder internationale Organisationen anzugeben sind.

23. Übermittlungen in Drittländer oder an internationale Organisationen:

Wenn es zu Übermittlungen an Empfänger in Drittländern oder an internationale Organisationen kommt, dann ist durch gesonderte Maßnahmen sicherzustellen, dass die personenbezogenen Daten geschützt werden.
Dies erfolgt durch „geeignete Garantien“, die in Art 46 DSGVO beschrieben sind, z.B. eine Vereinbarung mit dem Empfänger im Sinne sog. Standard-Vertragsklauseln (die von der EU-Kommission als „Mustervereinbarung“ erlassen werden).

24. Löschfristen:

Im Sinne der **(zeitlichen) Speicherbegrenzung**, dh dass personenbezogene Daten nur für eine bestimmte bzw. im Voraus bestimmbare Zeit von einer Organisation verarbeitet werden dürfen (siehe Art. 5 Abs 1 lit e DSGVO), ist es auch erforderlich, dass die Fristen für die (freiwillige und anlasslose) Löschung der Daten angegeben werden.
Dies kann eine absolute Frist sein oder eine Frist, die an ein bestimmtes Ereignis anknüpft, sodass die Art und Weise der Ermittlung des Endes der Verarbeitung der Daten.

Die Löschfristen sind dann anzugeben, wenn dies möglich ist (so der Text des Art 30 Abs 1 lit f DSGVO). Wenn es daher einfach möglich ist, die Löschfristen zu bestimmen, dann sollten diese möglichst konkret (z.B. 3 Jahre nach Ende der Vertragserfüllung …) angegeben werden. Wenn es schwierig ist, die konkrete Frist anzugeben, dann sollte beschrieben werden, unter welchen Voraussetzungen die Löschung erfolgt.

Die Fristen zur Löschung der personenbezogenen Daten ergeben sich z.B. aus vertraglichen Verpflichtungen zur Gewährleistung und/oder zur Leistung von Schadenersatz oder Aufbewahrungs- bzw. Speicherpflichten nach gesetzlichen Bestimmungen (z.B. 7 Jahre nach der Bundesabgabenordnung, 30 Jahre bei Krankenanstalten …)

25. Technische und organisatorische Maßnahmen:

Im Verzeichnis gem. Art 30 sind auch die **Maßnahmen aus technischer und organisatorischer Hinsicht** zu beschreiben, die zum **Schutz der personenbezogenen Daten** getroffen werden. Die Verpflichtung – nach bestimmten Kriterien – derartige Maßnahmen zu setzen, findet sich in Art 32 DSGVO, und dort findet sich auch ein Maßnahmenkatalog, der in demonstrativer Aufzählung (dh ohne Anspruch auf Vollständigkeit derartige Maßnahmen) beschreibt, z.B. Pseudonymisierung und Verschlüsselung. Daten und System sollen für den Normalbetrieb gerüstet sein, aber auch aus dem Gesichtspunkt der Sicherheit vor physischen oder technischen Zwischenfällen geschützt werden.

Unter diese Maßnahmen, die im Verzeichnis von Verarbeitungstätigkeiten zu beschreiben sind, fallen insbesondere auch eine **Rollenverteilung**, die **Auftragsbindung**, **Belehrung** und **Information** der Mitarbeiter über die Maßnahmen zum Datenschutz und die Verpflichtungen aus der DSGVO und dem DSG, Regelungen zu **Zutrittsberechtigungen** zu technischen Anlagen (Servern, Clients …) sowie ein **Berechtigungskonzept** in Bezug auf die Verarbeitung der personenbezogenen Daten (inkl. Passwort-Richtlinie) sowie eine **technische Absicherung** (Passwortschutz, Verschlüsselung) der Geräte, um einen unbefugten Zugriff zu verhindern sowie die **Zugriffsprotokollierung** der Verwendungsvorgänge.

Folgende **10 Maßnahmen** sind u.a. möglich bzw. sinnvoll:

Verwehrung des Zugangs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte (**Zugangskontrolle**)

Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Entfernens von Datenträgern (**Datenträgerkontrolle**)

Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten (**Speicherkontrolle**)

Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte (**Benutzerkontrolle**)

Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems

Berechtigten ausschließlich zu den ihrer Zugangsberechtigung unterliegenden personenbezogenen Daten Zugang haben (**Zugriffskontrolle**)

Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können (**Übertragungskontrolle**)

Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben worden sind (**Eingabekontrolle)**

Verhinderung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können (**Transportkontrolle**)

Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können (**Wiederherstellung**)

Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen, auftretende Fehlfunktionen gemeldet werden (Zuverlässigkeit) und gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können (**Datenintegrität**).

www.dataprotect.at
SMP Schweiger Mohr & Partner Rechtsanwälte OG
Huemerstraße 1 / Kaplanhofstraße 2, A-4020 Linz
ATU 40112014 Tel 0732/79 69 00 Fax 0732 796906
FN 37294w LG Linz / Österreich

Verfasser: RA Dr. Thomas Schweiger, LL.M. (Duke), CIPP/E