Schulungskompendium

Fragen und Antworten zur Risikoanalyse

Einführung in das MCSS Schulungskompendium

Das digitale MCSS Schulungs- und Einweisungs-System basiert auf den jeweils aktuellen Rahmenbedingungen für die Rechtskonformität in medizinischen Einrichtungen. Für die Anwendung der innovativen didaktischen Schulungen gelten folgende Richtlinien.

- Pro Frage sind etwa 1,5 – 2,0 Minuten aufzuwenden.
- Zuerst wird die Frage reflektiert und überlegt, welche Antworten gegeben werden können (evtl. mit schriftlichen Notizen).
- Anschließend werden die Überlegungen/Notizen mit den richtigen Antworten verglichen.
- Nach ca. 45 Minuten (ca. 20 Fragen und Antworten)sollte eine Konzentrationspause eingelegt werden.

Die Anwendung wird in MCSS protokolliert und die Anwendungsstatistik gilt als Nachweisdokument für die rechtlichen Audit Anforderungen.

Risikoanalyse in der Informationssicherheit

Basics RA + DSFA mit Beispielen

Weitere Dokumente: DSK KP 5, DSK KP 18, DSK Liste VAT (DSK = Datenschutzkonferenz)

Risikoanalyse in der Informationssicherheit

Welche Rahmenbedingungen gelten für die Risikoanalyse?

Art. 35 DSGVO

Datenschutz-Folgenabschätzung

(1) [1] Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so führt der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch. [2] Für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohen Risiken kann eine einzige Abschätzung vorgenommen werden.

(2) Der Verantwortliche holt bei der Durchführung einer Datenschutz-Folgenabschätzung den Rat des Datenschutzbeauftragten, sofern ein solcher benannt wurde, ein.

(3) Eine Datenschutz-Folgenabschätzung gemäß Absatz 1 ist insbesondere in folgenden Fällen erforderlich:

a) systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen;

b) umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Artikel 9 Absatz 1 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 oder

c) systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche;

(4) [1] Die Aufsichtsbehörde erstellt eine Liste der Verarbeitungsvorgänge, für die gemäß Absatz 1 eine Datenschutz-Folgenabschätzung durchzuführen ist, und veröffentlicht diese. [2] Die Aufsichtsbehörde übermittelt diese Listen dem in Artikel 68 genannten Ausschuss.

15	Anonymisierung von besonderen personenbezogenen Daten nach Artikel 9 DS-GVO nicht nur in Einzelfällen (in Bezug auf die Zahl der betroffenen Personen und die Angaben je betroffener Person) zum Zweck der Übermittlung an Dritte	Anonymisierung von besonderen Arten personenbezogener Daten nach Artikel 9	Umfangreiche besondere personenbezogene Daten werden durch ein Apothekenrechenzentrum oder eine Versicherung anonymisiert und zu anderen Zwecken selbst verarbeitet oder an Dritte weitergegeben.
16	Verarbeitung von personenbezogenen Daten gemäß Art. 9 Abs. 1 und Art. 10 DS-GVO - auch wenn sie nicht als „umfangreich“ im Sinne des Art 35 Abs. 3 lit. b) anzusehen ist - sofern eine nicht einmalige Datenerhebung mittels der innovativen Nutzung von Sensoren oder mobilen Anwendungen stattfindet und diese Daten von einer zentralen Stelle empfangen und aufbereitet werden.	Einsatz von Telemedizin-Lösungen zur detaillierten Bearbeitung von Krankheitsdaten	Ein Arzt nutzt ein Webportal oder setzt eine App an, um mit Patienten mittels Videotelefonie zu kommunizieren und Gesundheitsdaten durch Sensoren beim Patienten (z.B. Blutzucker, Sauerstoffmaske,...) detailliert und systematisch zu erheben und zu verarbeiten.

(7) Die Folgenabschätzung enthält zumindest Folgendes:

a) eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen;

b) eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck;

c) eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen gemäß Absatz 1 und

d) die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass diese Verordnung eingehalten wird, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen wird.

§ 38 BDSG

Datenschutzbeauftragte nichtöffentlicher Stellen

(1) [1] Ergänzend zu Artikel 37 Absatz 1 Buchstabe b und c der Verordnung (EU) 2016/679 benennen der Verantwortliche und der Auftragsverarbeiter eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten, soweit sie in der Regel mindestens 20 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen. [2] Nehmen der Verantwortliche oder der Auftragsverarbeiter Verarbeitungen vor, die einer Datenschutz-Folgenabschätzung nach Artikel 35 der Verordnung (EU) 2016/679 unterliegen, oder verarbeiten sie personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung, haben sie unabhängig von der Anzahl der mit der Verarbeitung beschäftigten Personen eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten zu benennen.

Risikoanalyse in der Informationssicherheit

Was ist das Ziel der Risikoanalyse ?

Was ist das Ziel der Risikoanalyse?

Ziel:
Das Risiko für die Rechte und Freiheiten natürlicher Personen mit ihren personenbezogenen Daten zu bewerten und zu beschützen. Eindämmen von Risiken durch ergreifen geeigneter technischer und organisatorischer Maßnahmen.

Risikoanalyse in der Informationssicherheit

Wie läuft die Risikoanalyse ab?

Wie läuft die Risikoanalyse ab ?

Folgende Phasen sind zu durchlaufen:

1. Risikoidentifikation
2. Abschätzung der Eintrittswahrscheinlichkeit und Schwere der möglichen Schäden
3. Zuordnung zu Risikoabstufungen

Risikoanalyse in der Informationssicherheit

Wie werden Risiken identifiziert ?

Wie werden Risiken identifiziert ?

1. Welche Schäden können für die natürlichen Personen auf der Grundlage der zu verarbeitenden Daten bewirkt werden?

Beispiele:
Diskriminierung, finanzieller Verlust, Rufschädigung, wirtschaftliche oder gesellschaftliche Nachteile, Ausschluss oder Einschränkung der Ausübung von Rechten und Freiheiten etc..

Risiko-Identifikation (2)

2. Wodurch, das heißt durch welche Ereignisse, kann es zu einem Schaden kommen?

Beispiele:

- Unbefugte oder unrechtmäßige Verarbeitung
- Verarbeitung wider Treu und Glauben
- Intransparente Verarbeitung
- Unbefugte Offenlegung von und Zugang zu Daten
- Unbeabsichtigter Verlust
- Zerstörung oder Schädigung von Daten
- Verarbeitung nicht richtiger Daten
- Verarbeitung über die Speicherfrist hinaus
- „Nichteinhaltung der Datenschutzgrundrechte/Betroffenenrechte“

Risiko-Identifikation (3)

3. Durch welche Handlungen und Umstände kann es zum Eintritt dieser Ereignisse kommen?
(Risikoquellen)

Beispiele:

- Durch Verantwortliche, Auftragsverarbeiter, Beschäftigte, ehemalige Mitarbeiter, Kunden/Interessenten oder Unbefugte die Zutritt erhalten haben
- Dies kann unbewusst passieren oder vorsätzlich und im eigenen Interesse
- Durch Cyberkriminelle
- Mögliche Intentionen sind Wirtschaftsterror, finanzielle Interessen, Wettbewerb etc.
- Durch sonstige Ereignisse, wie technische Fehlfunktionen (Provider), höhere Gewalt etc.

Risikoanalyse in der Informationssicherheit

Wie werden Eintrittswahrschein-lichkeiten und mögliche Schäden ermittelt ?

Wie werden Eintrittswahrscheinlichkeiten und mögliche Schäden ermittelt ?

Mit welcher Wahrscheinlichkeit tritt ein bestimmtes Ereignis ein?
(sorgloser Umgang von Beschäftigten, technische Fehlfunktion, Ausspähung durch Dritte, unzureichende Vorkehrungen des Verantwortlichen durch Unwissenheit, Zeitmangel, Unvermögen etc.)

Die Schwere des Schadens ermitteln.
(Schadensklasse, Schadenshöhe, Reputation, weitere Auswirkungen)

Eintrittswahrscheinlichkeit + Schäden (2)

Definition Risiko:
In der ISO 31000, dem ISO Standard für das Risikomanagement (Risk management – Principles and guidelines) oder der ISO/IEC 27001 – Managementsystem für Informationssicherheit, ist das Risiko folgendermaßen definiert:

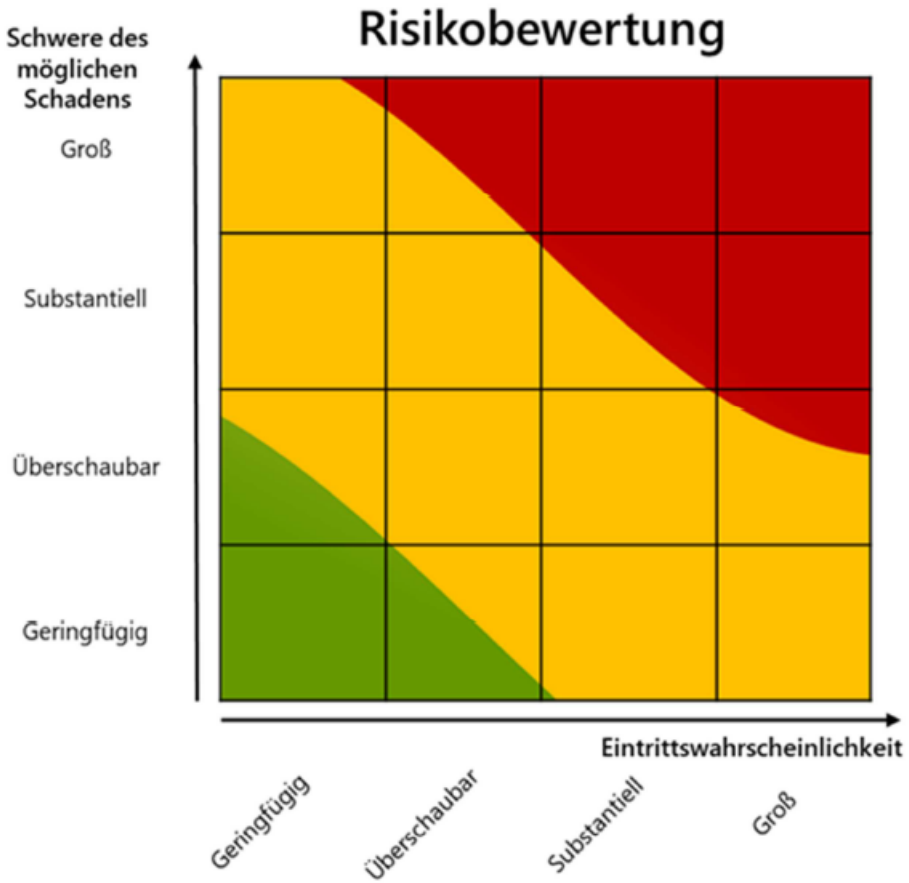
Risiko = Schaden x Eintrittswahrscheinlichkeit

Das Risiko ist das Produkt aus dem potentiell möglichen Schaden und der damit verbunden Eintrittswahrscheinlichkeit.
Um Schaden und Eintrittswahrscheinlichkeit miteinander multiplizieren zu können, müssen wir sie in Werte „umwandeln“ bzw. klassifizieren.

Risikoanalyse in der Informationssicherheit

Wie können Risiken kategorisiert werden?

Wie können Risiken kategorisiert werden?



Zuordnung zur Schadensklasse

Schadensklasse	Finanzieller Schaden	Ausfall Kernprozesse	Reputationsschaden	Auswirkungen auf natürliche Personen
gering	< 5.000 €	Minimale Verzögerungen in den nachfolgenden Prozessen (bis zu 2 Stunden)	Vorfall ist nur internen Mitarbeitern bekannt. Keine medialen Auswirkungen	Nachteile (wirtschaftlich, gesellschaftlich) im geringen Umfang für die Person
mittel	Zwischen 5.000 € und 20.000 €	Führt zu einer Verzögerung von ca. einen Tag bei den nachfolgenden internen Prozessen	Regionale mediale Auswirkungen	Finanzieller Schaden (nicht existenzgefährdend)

Schadensklasse	Finanzieller Schaden	Ausfall Kernprozesse	Reputationsschaden	Auswirkungen auf natürliche Personen
hoch	Zwischen 20.000 € und 50.000 €	Führt zu einer Verzögerung von mehr als einen Tag bei den nachfolgenden internen Prozessen	Vorfall hat nationale Mediale Auswirkungen, negatives Images auch bei Stellenausschreibungen	Identitätsdiebstahl, Diskriminierung
sehr hoch	> 50.000 €	Führt zu einer Verzögerung bei den geplanten Lieferzeiten; Kundentermine können nicht eingehalten werden	Vorfall hat internationale mediale Auswirkungen, Verlust von Kunden	Lebensgefahr, Existenzgefährdend

Risikoanalyse in der Informationssicherheit

Welche Konsequenzen ergeben sich aus der Risikoanalyse?

Welche Konsequenzen ergeben sich aus der Risikoanalyse?

Eine Risikoanalyse muss einem systematischen Aufbau folgen.
Die Ergebnisse müssen reproduzierbar sein. Würde eine andere Person mit gleichem Know-How dasselbe Risiko bewerten, sollte es anhand der objektiven Kriterien zum selben Ergebnis kommen.

Eine Risikoanalyse ermittelt die Risiken und Gefahren.
Dies führt bei niedrigen Risiken zu einem vereinfachten Verfahren (AV-Vertrag, sonstige Maßnahmen) und bei höheren Risiken zu einer Datenschutzfolgeabschätzung DSFA mit Maßnahmen zur Risikoeindämmung (notfalls Behörden einschalten).