Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Anstalt des öffentlichen Rechts

Sommerakademie 2016

DATENSCHUTZ NEU DENKEN!

(Neue) Anforderungen der Datenschutz-Grundverordnung für die IT-Sicherheit

Heiko Behrendt
ISO 27001 Auditor
Fon: 0431 988 1212
Mail: behrendt@datenschutzzentrum.de
Web: https://www.datenschutzzentrum.de/

Themen

- Aufbau der DSGVO
- Vorschriften in Bezug auf die IT-Sicherheit
- Anforderungen mit Handlungsnotwendigkeiten
- 10 Punkteplan für die Umsetzung

Datenschutz-Grundverordnung

Kapitel

- 99 Artikel
- Kapitel 1 Allgemeine Bestimmungen
- Kapitel 2 Grundsätze
- Kapitel 3 Rechte der Betroffenen Person
- Kapitel 4 Verantwortlicher und Auftragsverarbeiter
- Kapitel 5 Übermittlung personenbezogener Daten an Drittländer oder an internationale Organisationen
- Kapitel 6 Unabhängige Aufsichtsbehörden
- Kapitel 7 Zusammenarbeit und Kohärenz
- Kapitel 8 Rechtsbehelfe, Haftung und Sanktionen
- Kapitel 9 Vorschriften für besondere Verarbeitungssituationen
- Kapitel 10 Delegierte Rechtsakte und Durchführungsrechtsakte
- Kapitel 11 Schlussbestimmungen

Vorschriften in Bezug auf die IT-Sicherheit

in Kraft seit 25. Mai 2016 – gilt ab 25. Mai 2018

- Artikel 5 Grundsätze für die Verarbeitung personenbezogener Daten
- Artikel 24 Verantwortung des für die Verarbeitung Verantwortlichen
- Artikel 25 Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen
- Artikel 28 Auftragsverarbeiter
- Artikel 30 Verzeichnis von Verarbeitungstätigkeiten
- Artikel 32 Sicherheit der Verarbeitung
- Artikel 33 Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde
- Artikel 34 Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person
- Artikel 35 Datenschutz-Folgenabschätzung
- Artikel 37 Benennung eines Datenschutzbeauftragten (Öffnungsklausel).: Entwurf ABDSG § 14)
- Artikel 58 Befugnisse (Aufsichtsbehörde)

Artikel 5

Grundsätze für die Verarbeitung personenbezogener Daten

Maßstab für die Datensicherheit!

- § Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz
- § Zweckbindung – Verarbeitung für eindeutige und legitime Zwecke
- § Datenminimierung – auf das notwendige Maß beschränkt
- § Richtigkeit – Berichtigung oder Löschung unrichtiger Daten
- § Speicherbegrenzung – Löschung der Daten
- § Integrität und Vertraulichkeit – angemessene Sicherheit durch TOMs
- § Rechenschaftspflicht – **Nachweis** für die Einhaltung der Grundsätze

✓ **Sicherheitskonzept**

Artikel 24

Verantwortung des für die Verarbeitung Verantwortlichen

Festlegung des Schutzniveaus!

- „Der Verantwortliche setzt unter Berücksichtigung **der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung** sowie der unterschiedlichen **Eintrittswahrscheinlichkeit und schwere der Risiken** für die Rechte und Freiheiten natürlicher Personen geeignete **technische und organisatorische Maßnahmen** um, um sicherzustellen und den **Nachweis** dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt.“

- „Die Maßnahmen werden erforderlichenfalls überprüft und aktualisiert.“

- Nachweis kann durch eine Zertifizierung erbracht werden.

✓ **Technische Unterlagen, Schutzbedarfsfeststellung**

Artikel 25

Datenschutz durch Technikgestaltung und durch Voreinstellungen

Umsetzung der Datensicherheit vor Inbetriebnahme!

- § „Der Verantwortliche trifft sowohl **zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete technische und organisatorische Maßnahmen.“**

- § „Der Verantwortliche trifft durch **Voreinstellung** geeignete **technische und organisatorische Maßnahmen**, die sicherstellen, dass grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden.“

- § Nachweis kann durch eine Zertifizierung erbracht werden.

- ✓ **Maßnahmenkatalog für die Datenverarbeitung**

Artikel 28
Auftragsverarbeiter

Der Auftragsverarbeiter muss die Umsetzung der DSGVO nachweisen!

§ „Erfolgt eine Verarbeitung im Auftrag eines Verantwortlichen, so arbeitet dieser nur mit Auftragsverarbeitern, die hinreichend **Garantien** dafür bieten, **dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt** und den Schutz der Rechte der betroffenen Person gewährleistet.“

§ Nachweis kann durch eine Zertifizierung erbracht werden.

✓ **Vertrag mit Sicherheitskonzept, ggf. ISO 27001 Zertifikat**

Artikel 30

Verzeichnis von Verarbeitungstätigkeiten

Kontrolle der Verarbeitungsvorgänge!

§ „Jeder Verantwortliche und gegebenenfalls sein Vertreter führen ein **Verzeichnis** aller **Verarbeitungstätigkeiten**, die ihrer Zuständigkeit unterliegen.“

§ „Jeder **Auftragsverarbeiter** und gegebenenfalls sein Vertreter führen ein Verzeichnis zu allen Kategorien von im Auftrag eines Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung.“

§ Meldepflicht gegenüber der Aufsichtsbehörde entfällt.

✓ **Verfahrensverzeichnis**

Artikel 32

Sicherheit der Verarbeitung

Technische und organisatorische Maßnahmen unter Berücksichtigung des Stands der Technik nach Festlegung des Schutzniveaus und der Durchführung einer Risikoanalyse bestimmen und umsetzen!

§ „Unter Berücksichtigung des **Stands der Technik**, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen **Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen** treffen der Verantwortliche und der Auftragsverarbeiter geeignete **technische und organisatorische Maßnahmen**, um ein dem **Risiko angemessenes Schutzniveau** zu gewährleisten.“

✓ **Schutzbedarfsfeststellung, Maßnahmenkatalog, Risikoanalyse**

Artikel 33

Meldung von Verletzungen des Schutzes personenbezogener Daten

Datenschutzvorfälle innerhalb von 72 Stunden melden!

- „Im Falle einer **Verletzung des Schutzes personenbezogener Daten** meldet der Verantwortliche unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der zuständigen **Aufsichtsbehörde**, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.“
- Keine Begrenzung auf sensible Daten.
- Auftragsverarbeiter melden an den Verantwortlichen (Auftraggeber).

✓ **Datenschutz- und Sicherheits(vorfall)management**

Artikel 34

Benachrichtigung der von einer Verletzung ... betroffenen Personen

Meldung an betroffene Personen bei hohem Risiko!

§ „Hat die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein **hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen** zur Folge, so benachrichtigt der Verantwortliche die betroffene Person unverzüglich von der Verletzung.“

§ Beschreibung des Datenschutzvorfalls und der ergriffenen Maßnahmen zur Behebung.

✓ **Datenschutz- und Sicherheits(vorfall)management**

Artikel 35

Datenschutz-Folgenabschätzung

Risikoanalyse vor Inbetriebnahme der Verarbeitung!

- „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.“

- Beschreibung der Verarbeitungsvorgänge, Bewertung der Notwendigkeit und Verhältnismäßigkeit, Bewertung der Risiken, Abhilfemaßnahmen, Garantien als Nachweis zur Einhaltung der DSGVO.

✓ **Datenschutzmanagement, (Rest-)Risikoanalyse**

Artikel 37

Benennung eines Datenschutzbeauftragten

Datenschutzbeauftragter?!

§ „Der Verantwortliche und der Auftragsverarbeiter benennen auf jeden Fall einen Datenschutzbeauftragten, wenn

a) die Verarbeitung von **einer Behörde oder öffentlichen Stelle** durchgeführt wird,

b) regelmäßige und **systematische Überwachung** von betroffenen Personen,

c) Verarbeitung **besonderer Kategorien von Daten** gemäß Artikel 9.

§ **ABDSG Entwurf 05.08.2016:** Das Gleiche gilt für Verantwortliche und Auftragsverarbeiter, soweit sie in der Regel mindestens zehn Personen ständig mit der Verarbeitung personenbezogener Daten beschäftigen.

Artikel 58
Befugnisse

Aufsichtsbehörde bekommt mehr Befugnisse!

- **Untersuchungsbefugnisse**
  - Datenschutzprüfungen
  - Überprüfungen von Zertifizierungen
  - Zugang zu allen Informationen

- **Abhilfebefugnisse – Sanktionsrahmen**
  - Geldbuße, wenn Verarbeitungsvorgänge gegen die Verordnung verstoßen, **auch bei unzureichenden TOMs**
  - Anweisung über die Beseitigung von Mängeln in einer vorgegebenen Frist
  - **Beschränkung oder Verbot der Datenverarbeitung verhängen**

Umsetzung der Datenschutzvorschriften (DSGVO)

10 Punkteplan!

1. Entscheidung für die Anwendung eines qualifizierten Sicherheitsstandards (ISO 27001 native oder IT-Grundschutz mit DSGVO)
2. Implementierung eines Datenschutz- und Sicherheitsmanagements
3. Angemessener Einsatz personeller und fachlicher Ressourcen
4. Sensibilisierung und Schulung aller Mitarbeiter
5. Bestandsaufnahme der Datenverarbeitung und Geschäftsprozesse
6. Ermittlung des Schutzniveaus der Daten mit Risikoanalyse
7. Festlegung und Umsetzung von Schutzmaßnahmen (TOMs)
8. Nachweis: Dokumentation der IT-Systeme und der Datenverarbeitungsvorgänge in einem Datenschutz- und Informationssicherheitskonzept
9. Überprüfung und Kontrolle auf Einhaltung der TOMs und der DSGVO
10. Zertifizierung als „garantierter“ Nachweis zur Einhaltung der DSGVO

DATENSCHUTZ NEU DENKEN!

Vielen Dank für Ihre Aufmerksamkeit!

Heiko Behrendt
ISO 27001 Auditor
Fon: 0431 988 1212
Mail: behrendt@datenschutzzentrum.de
Web: https://www.datenschutzzentrum.de/