klöschinski
it-lösungen

STEUERBERATERVERBAND
RHEINLAND-PFALZ e.V.

Alles neu macht der Mai

Die neue DSGVO

klöschinski
it-lösungen

Alles neu macht der Mai 2018

„Die EU-Datenschutz-Grundverordnung ist künftig DAS einheitliche, starke Datenschutzgesetz für alle 500 Millionen BürgerInnen der Europäischen Union. Sie schafft Transparenz, gibt den VerbraucherInnen auf dem gesamten EU-Binnenmarkt durchsetzbare Rechte und sorgt für faire Wettbewerbsbedingungen sowie Rechtssicherheit auf Seiten der Unternehmen. Die Verordnung löst den Flickenteppich vorheriger Regelungen in den 28 Mitgliedstaaten ab.“

klöschinski
it-lösungen

Bin ich betroffen?

- Kanzleien **jeder** Größe müssen sich mit der DSGVO beschäftigen

- **Jedoch nicht alle benötigen einen Datenschutzbeauftragten!**
- Ergänzend zu Artikel 37 DSGVO regelt der § 38 BDSG (neu) den Datenschutzbeauftragten nichtöffentlicher stellen (soweit Sie i.d.R. mindestens zehn Personen **ständig mit der automatisierten Verarbeitung** personenbezogener Daten beschäftigen).

klöschinski
it-lösungen

Benennung eines fachkundigen Datenschutzbeauftragten

Der Datenschutzbeauftragte muss…

… fachkundig sein.

- Fachwissen im Datenschutzrecht
- Fachwissen in der Datenschutzpraxis
- Grundlage ist die berufliche Qualifikation

… zuverlässig sein.

- Die Wahrnehmung anderer Pflichten darf nicht zu einem Interessenkonflikt führen.

… in der Lage sein, seine Aufgaben zu erfüllen.

- Unterrichtung und Beratung des Verantwortlichen und der Beschäftigten
- Überwachung der Einhaltung des Gesetzes, der Strategien zum Datenschutz, der Zuweisung von Zuständigkeiten und der Schulungen
- Beratung bei der Datenschutz-Folgenabschätzung
- Zusammenarbeit mit der Aufsichtsbehörde
- Ansprechpartner der Aufsichtsbehörde

Die Ressourcen hierfür muss das Unternehmen bereitstellen!

klöschinski
it-lösungen

Was ändert sich technisch? „TOM's"

Bisher, die acht goldenen Regeln:

- 1 Zutrittskontrolle
- 2 Zugangskontrolle
- 3 Zugriffskontrolle
- 4 Weitergabekontrolle
- 5 Eingabekontrolle
- 6 Auftragskontrolle
- 7 Verfügbarkeitskontrolle
- 8 Trennungskontrolle

Erforderlich sind Maßnahmen, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

klöschinski
it-lösungen

Künftig

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; diese Maßnahmen schließen unter anderem Folgendes ein:

klöschinski
it-lösungen

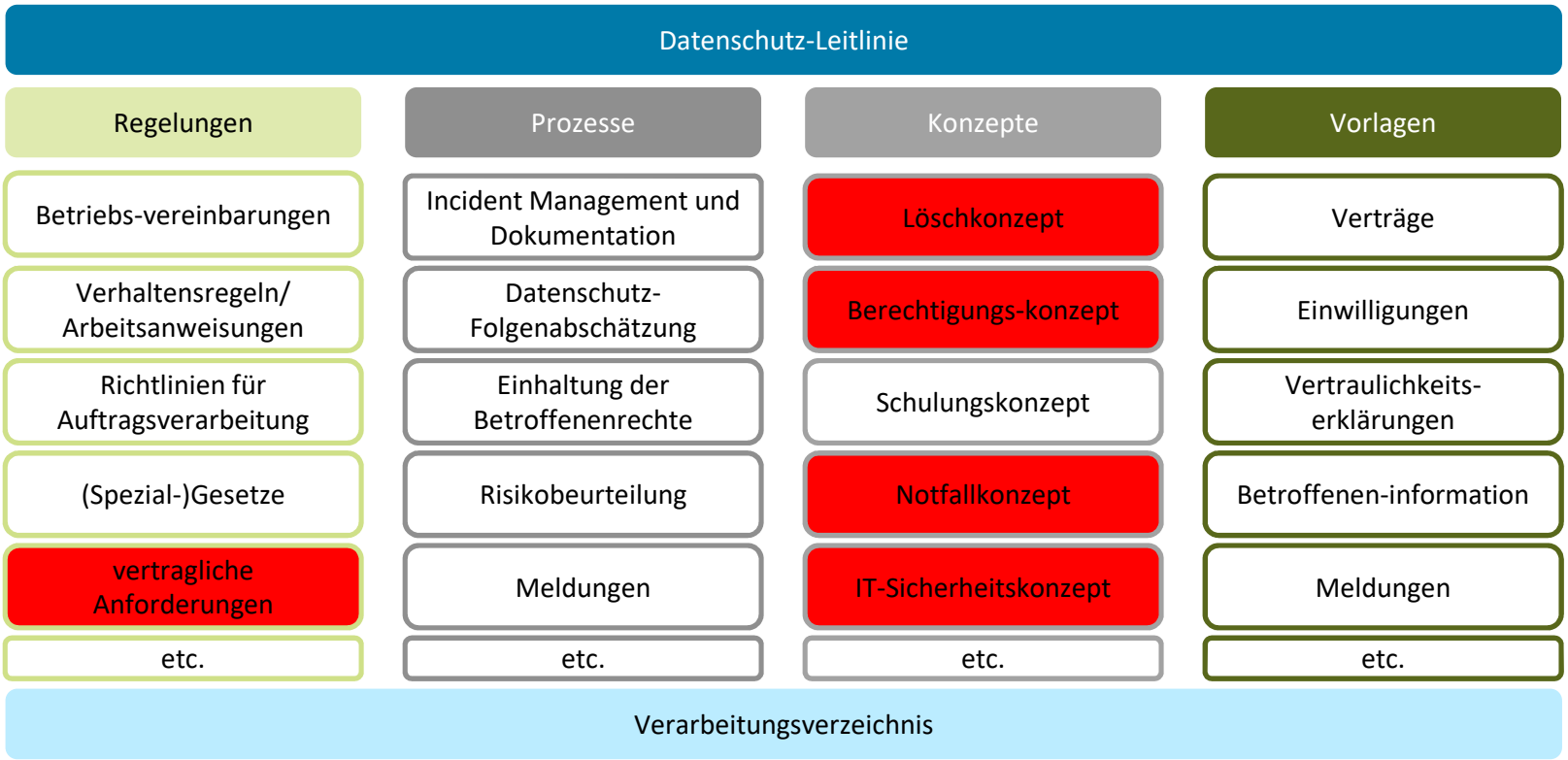
Künftig: konkrete Regelbeispiele

- die Pseudonymisierung und Verschlüsselung personenbezogener Daten – **Ordner-Rücken**
- die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen – **IT-Monitoring**
- die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen – **Datensicherungskonzept**
- ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

  Prüfung der IT Umgebung (Grundschutzhandbuch)

klöschinski
it-lösungen

Datenschutz-Management-System aufbauen



klöschinski
it-lösungen

Vertragliche Anforderungen

„Auftragsdatenverarbeitung“

„Auftragsverarbeitung“

klöschinski
it-lösungen

Auftragsverarbeitung überprüfen!

- Was sind Auftragsverarbeiter?

→ Jeder, der Daten im Auftrag und auf Weisung des Verantwortlichen verarbeitet, z. B.

System-Partner	DATEV	Aktenvernichter	Abrechnungsbüros
Rechenzentren/ Cloud Computing	Wartung von Telefonanlagen	Wartung von Multi-funktionsgeräten	Office-Dienstleister

- Auftragsverarbeitung ist grundsätzlich erlaubt, sofern die Anforderungen der EU-Datenschutz-Grundverordnung erfüllt sind:
  - sorgfältige Auswahl
  - Vertrag (auch elektronisch)
  - Arbeiten nur auf dokumentierte Weisung
  - **Umsetzung von TOMs**

- Unterstützung des Verantwortlichen bei der Erfüllung seiner Pflichten
- Regelung von Unterauftragsverhältnissen
- Verpflichtung der Mitarbeiter zu Vertraulichkeit
- Überprüfungen durch den Verantwortlichen

klöschinski
it-lösungen

Fazit

- Die DSGVO verlangt von allen Unternehmen im Bereich des Datenschutzes eine deutliche Professionalisierung insbesondere der Dokumentation und Datensicherheit.

klöschinski
it-lösungen

Zusammenfassung: Wo beginne ich? Technik!

- Sind die bisher 8 goldenen Regeln erfüllt?
  - (Dokumentation der Prozesse hinsichtlich IT- Sicherheit, Datensicherung, ….)
  - Bisherige Schutzmaßnahmen sind nicht notwendigerweise „falsch“, aber sie müssen nach diesen Prinzipien überprüft und es muss der Nachweis der Angemessenheit (Nachweispflicht gem. Art. 5 Abs. 2 DS-GVO) geführt werden.
- Habe ich Verträge zur Auftragsdatenverarbeitung geschlossen?

Vielen Dank für Ihre Aufmerksamkeit!

klöschinski ASP
IT-Outsourcing. Freiräume schaffen.

Markus Hamm
mhamm@kl-it.de