Datenschutzmanagement messbar machen und so strukturiert weiterentwickeln

Warum Datenschutzorganisationen nach einem Standard mit Reifegradmodell aufgesetzt werden sollten

Vorwort

Standardisiertes Datenschutzmanagement ermöglicht:

- Systematische Identifikation von Schwachstellen und Verbesserungspotenzialen
- Messbare Fortschritte und vergleichbare Ergebnisse
- Motivationsinstrument durch Sichtbarmachung von Entwicklungen
- Benchmarking zwischen Abteilungen und Standorten

Themen heute

Fokus auf Aufbau, Optimierung und Messung eines DSMS nach:

IDW 9.860.1 Standard

Reifegradmodell

KPIs zur Erfolgsmessung

Ein unterlegtes Modell zur Risikobewertung zur Priorisierung notwendiger Maßnahmen

Vorteile eines Reifegradorientierten DSMS

Ergebnisse können regelmäßig überprüft werden.

Fortschritte in der Umsetzung und Wirksamkeit von Maßnahmen werden messbar.

Ziel:

Kontinuierliche Verbesserung der Datenschutzpraktiken des Unternehmens.

Vorstellung des IDW 9.860.1

Ein vom Institut der Wirtschaftsprüfer in Deutschland e.V. (IDW) entwickelter Standard ermöglicht die Prüfung von IT-Systemen zu planen, durchzuführen sowie darüber Bericht zu erstatten

Prüfungshinweise der Anlage 1 sind spezifische Konkretisierungen dieses Standards, die sich auf das zugrundeliegende Datenschutz-Managementsystem beziehen

IDW 9.860.1 orientiert sich entlang der europäischen und deutschen gesetzlichen Anforderungen, die sich für nicht-öffentliche Stellen aus der Datenschutz-Grundverordnung (DSGVO) und dem Bundesdatenschutzgesetz (BDSG) ergeben

Der Anforderungskatalog des IDW PS 860 konkretisiert diese Regelungen im Kontext der Verarbeitung personenbezogener Daten und stellt geeignete Kriterien für die Beurteilung der datenschutzspezifischen Maßnahmen dar, die von der jeweiligen nicht-öffentlichen Stelle getroffen wurden

Der IDW PH 9.860.1 gliedert Anforderungen unter folgenden Überschriften, beschreibt diese im Detail und ordnet ihnen die einschlägigen Artikel der DSGVO zu.

1. Aufbau- und Ablauforganisation
2. Datenschutzbeauftragter
3. Datenschutzrechtliches Risikomanagement
4. Rechtmäßigkeit (Zulässigkeit) der Verarbeitungen
5. Verzeichnis der Verarbeitungstätigkeiten
6. Privacy by Design & by Default
7. Technische und organisatorische Maßnahmen
8. Zweckbindung der Verarbeitungstätigkeiten und Löschmanagement
9. Management der Betroffenenrechte
10. Management von Datenschutzverletzungen
11. Management der Auftragsverarbeiter
12. Management der Drittlandübermittlungen

Vorbereitung und Anpassung

1. **Einheitliche Grundlagen schaffen:**
   Mit der Planung des Vorhabens betrauten Mitarbeitende sollten Grundsätze des IDW PS 980 für die Planung und Durchführung einer Prüfung von Compliance Management Systemen verstehen.

2. **Vertrautheit mit den Anforderungen des Unternehmens sicherstellen und unternehmensspezifische Anpassungen durchführen:**
   Die spezifischen Gegebenheiten und Bedürfnisse des Unternehmens müssen verstanden sein - einschließlich der Art der Datenverarbeitung und des Risikoprofils - um dies in die Gewichtung der Prüfungshandlungen einzuarbeiten.
   All das unter Einbeziehung der Informationssicherheit und Berücksichtigung weiterer gesetzlicher oder regulatorischer Datensc hutzanforderungen, insbesondere bei Unternehmen mit Standorten in nicht-europäischen Staaten angepasst werden.

3. **Klares Bild des "Soll" und "Ist" anstreben:**
   In der Ausgestaltung der Prüfung muss grösster Wert auf die Beschreibung des klaren "Solls" der einzelnen Aspekte eines Datenschutz-Managementsystems sowie der Datenschutzorganisation gelegt werden.
   Ziel ist die Sicherstellung, dass mittels einer verständlichen Beschreibung ein verwertbarer Abgleich mit dem vorgefundenen "Ist-Zustand" erfolgen kann.

4. **Aussagekraft erhalten:**
   Die hohe Aussagekraft des IDW PH 9860.1 sollte im angepassten Prüfkatalog, hinsichtlich der durchzuführenden Prüfungshandlungen, Prüfungsfeststellungen, Empfehlungen und weiteren Erläuterungen beibehalten werden.

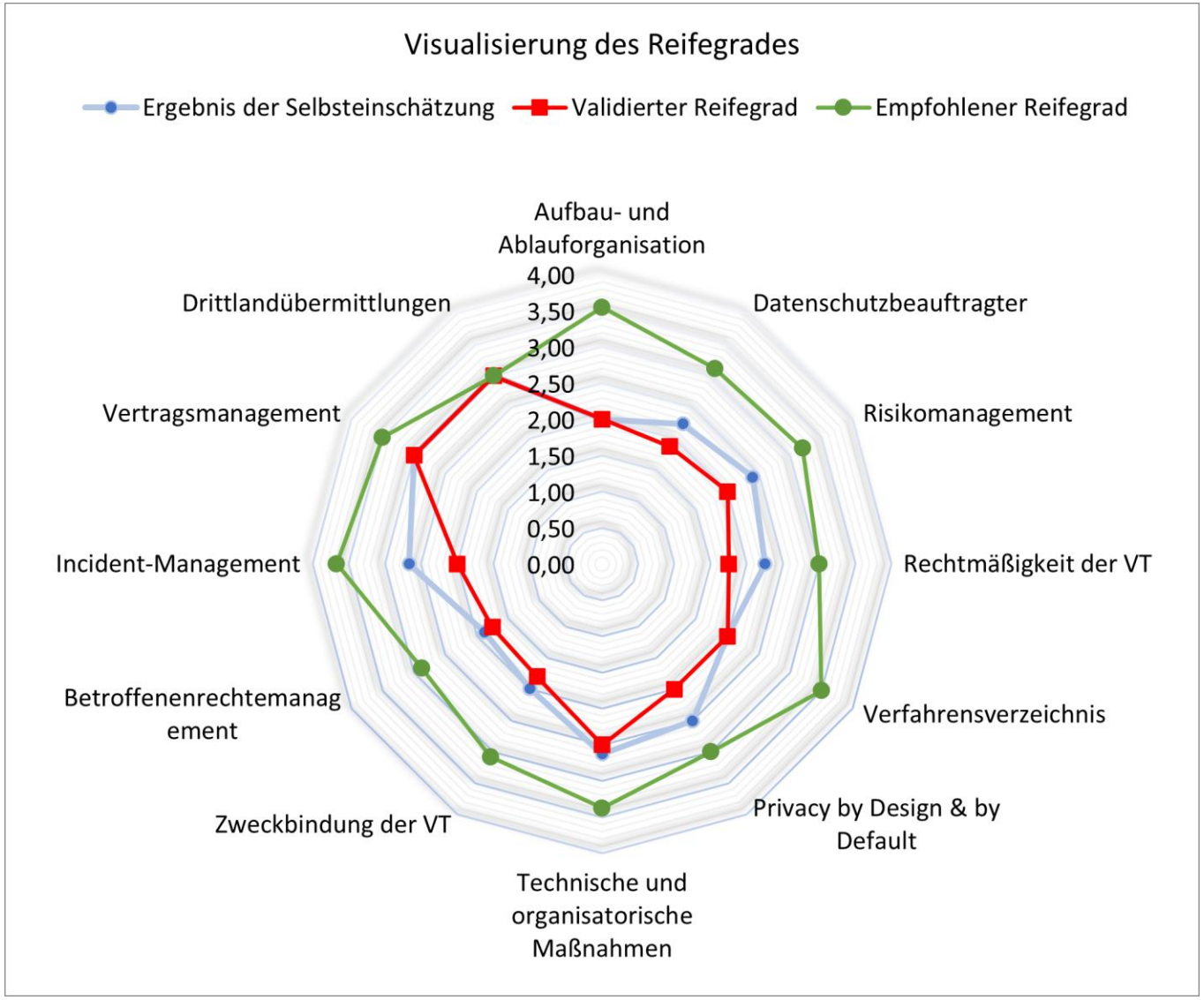
5. **Klare Beschreibungen der Nachweise**:
   Durch konkret formulierte Anforderungen ist sicherzustellen, dass klare Beschreibungen der Nachweise vorliegen
   (bspw. Richtlinien, Arbeitsanweisungen, Verfahrensanweisungen, Prozessdokumentationen, Verzeichnisse oder Schulungskonzepte, in denen zentrale Vorgaben zur Durchführung, zum Ablauf und zu den Verantwortlichkeiten schriftlich geregelt sind)

6. **Berücksichtigung von BCR oder COC:**
   Sofern gegeben, sollten diese mit den Anforderungen in Begrifflichkeit und Struktur abgeglichen werden, bzw. die Struktur in die Prüffragen eingearbeitet werden

Reifegradmodelle beschreiben die Stabilität und Leistungsfähigkeit des DSMS

Nutzen:

- Schwachstellen identifizieren
- Verbesserungspotenziale aufzeigen
- Motivation durch Fortschritte bei wiederholten Prüfungen



Gamification

- Vergleich von Fachbereichen oder Standorten über Management-Berichte oder Compliance-Dashboards
- Gamification zur Förderung der Reife der Datenschutzorganisationen nutzen

KPI – Key Performance Indicators

- Abfragen für Leistungskennzahlen können mit den Kontrollen nach IDW 9.860.1 verknüpft werden.
- Je nach Grösse oder Struktur des Unternehmens können diese Leistungskennzahlen auf Standorte, Niederlassungen oder Bereiche heruntergebrochen werden.

4 Beispiele

1. Datenschutzschulungen

Referenz im IDW:
Nr. 1 – Aufbau- und Ablauforganisation – Nr. 9

- ✓Wie viele allgemeinen Datenschutzschulungen, die Grundlagen des Datenschutzes betreffend, sind im Zeitraum * durchgeführt worden?
- ✓Wie viele bereichs- oder themenspezifische Datenschutzschulungen sind im Zeitraum * durchgeführt worden?

2. Risikomanagement

Referenz im IDW:
Nr. 3 – Datenschutzrechtliches Risikomanagement – Nr. 29

- ✓Wie viele Verarbeitungstätigkeiten wurden im Zeitraum * durch den/die Datenschutzbeauftragte:n kontrolliert?
- ✓In wie vielen Fällen gab es konkrete Beanstandungen?
- ✓Bei wie vielen Fällen konnten keine zufriedenstellenden Abhilfemaßnahmen geschaffen werden?

3. Betroffenenrechte

Referenz im IDW:
Nr. 9 – Betroffenenrechte – Nr. 64, 66

- ✓Wie viele Anfragen Betroffener sind im Zeitraum * bei der Datenschutzorganisation / über das Portal eingegangen?
- ✓Wie viele davon betrafen
  - ✓Auskunftsrechte gem. Art. 15 DS-GVO
  - ✓ Löschersuchen gem. Art. 17 DS-GVO
  - ✓In wie vielen Fällen konnte innerhalb der gesetzlich vorgegebenen Frist von 4 Wochen eine vollständige Auskunft nach Art. 15 DS-GVO erteilt werden?

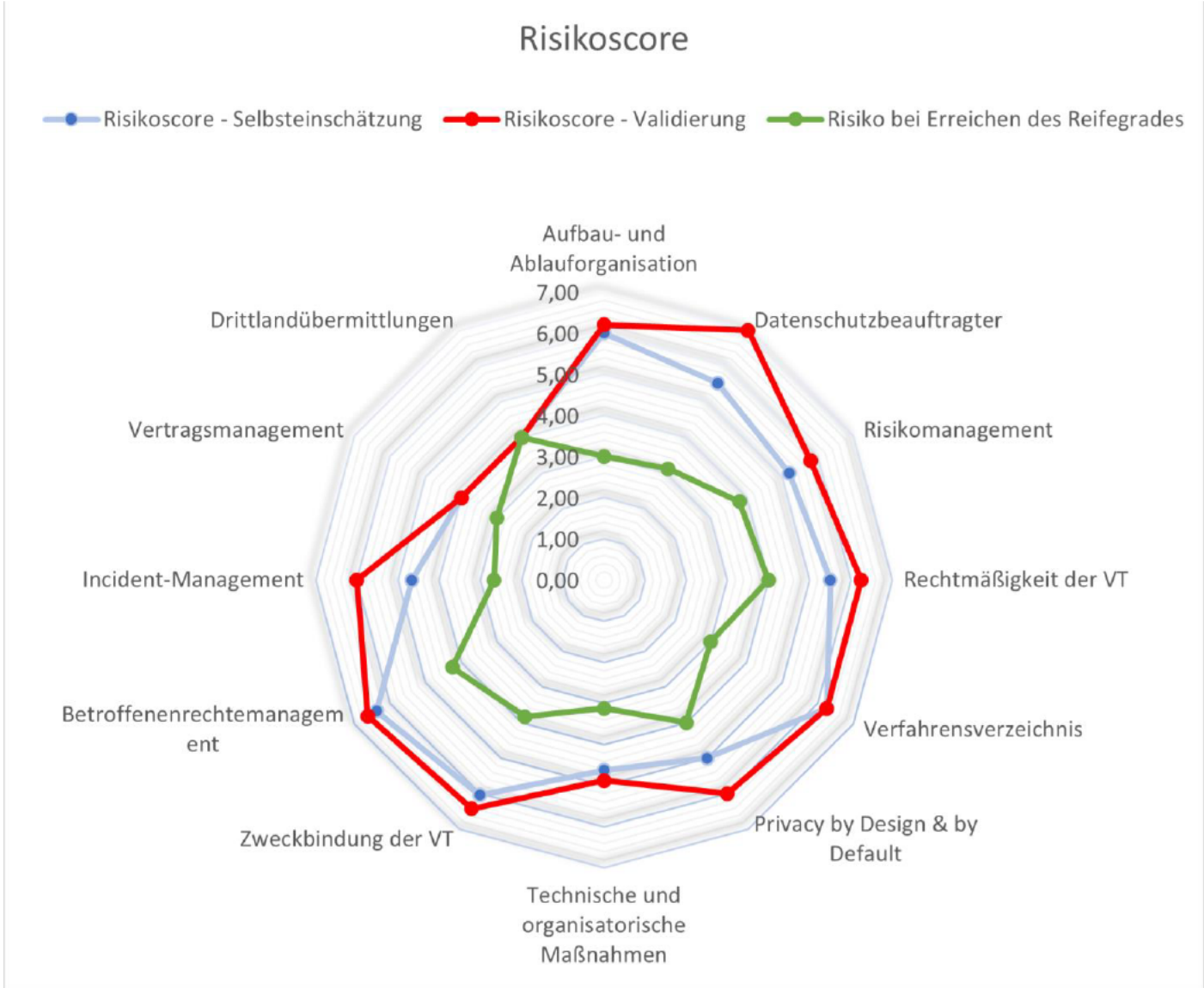
4. Datenschutzverletzungen

Referenz im IDW:
Nr. 10 – Incident Management – Nr. 71ff

- ✓ Wie viele Meldungen von Schutzverletzungen gem. Art. 4 Abs. 12 DS-GVO sind im Zeitraum * bei der Datenschutzorganisation / über das Portal * eingegangen?
- ✓ Wie viele Meldungen von Schutzverletzungen sind von einem der eigenen Auftragsverarbeiter ausgegangen?
- ✓ In wie vielen Fällen konnte innerhalb der gesetzlich vorgegebenen 72h eine Entscheidung über die Meldeerfordernis auf Basis vollständiger Angaben gem. Art. 33 DS-GVO getroffen werden?
- ✓ Wie viele Meldungen wurden bei der zuständigen Aufsichtsbehörde im Zeitraum * abgegeben?
- ✓ Wie oft wurden Betroffene gem. Art. 34 DS-GVO im Zeitraum * benachrichtigt?

Risikomanagement

- Hilfreich: Priorisieren der Vielzahl an aufgezeigten Maßnahmen im Rahmen einer Risikobewertung.
- Interessanter Nebenaspekt: Hier gewonnene Werte können auch in Berichte für das interne Risikomanagement einfließen, bzw. nach einer sinnvollen „Übersetzung“ nutzbar gemacht werden.
- Für die Übersetzung sollten die Sanktionspraktiken des jeweiligen Landes ebenso berücksichtigt werden, wie aktuelle Entwicklungen bei Klagen von bspw. Verbraucherschutzverbänden oder einzelnen Betroffenen.



Fazit

- Datenschutzmanagement ist nicht nur gesetzliche Pflicht, sondern auch eine Frage der Effizienz.
- Ein optimiertes Datenschutzmanagementsystem:
  - Minimiert Risiken von Datenschutzverletzungen
  - Stärkt das Vertrauen von Beschäftigten, Management und Shareholdern

Nachzulesen unter:
Springer Verlag
IT-Prüfung, Datenschutzmanagement und KI-Audit: Neue Ansätze für die IT-Revision Taschenbuch – 13. März 2025 – von Aleksandra Sowa (Herausgeber)