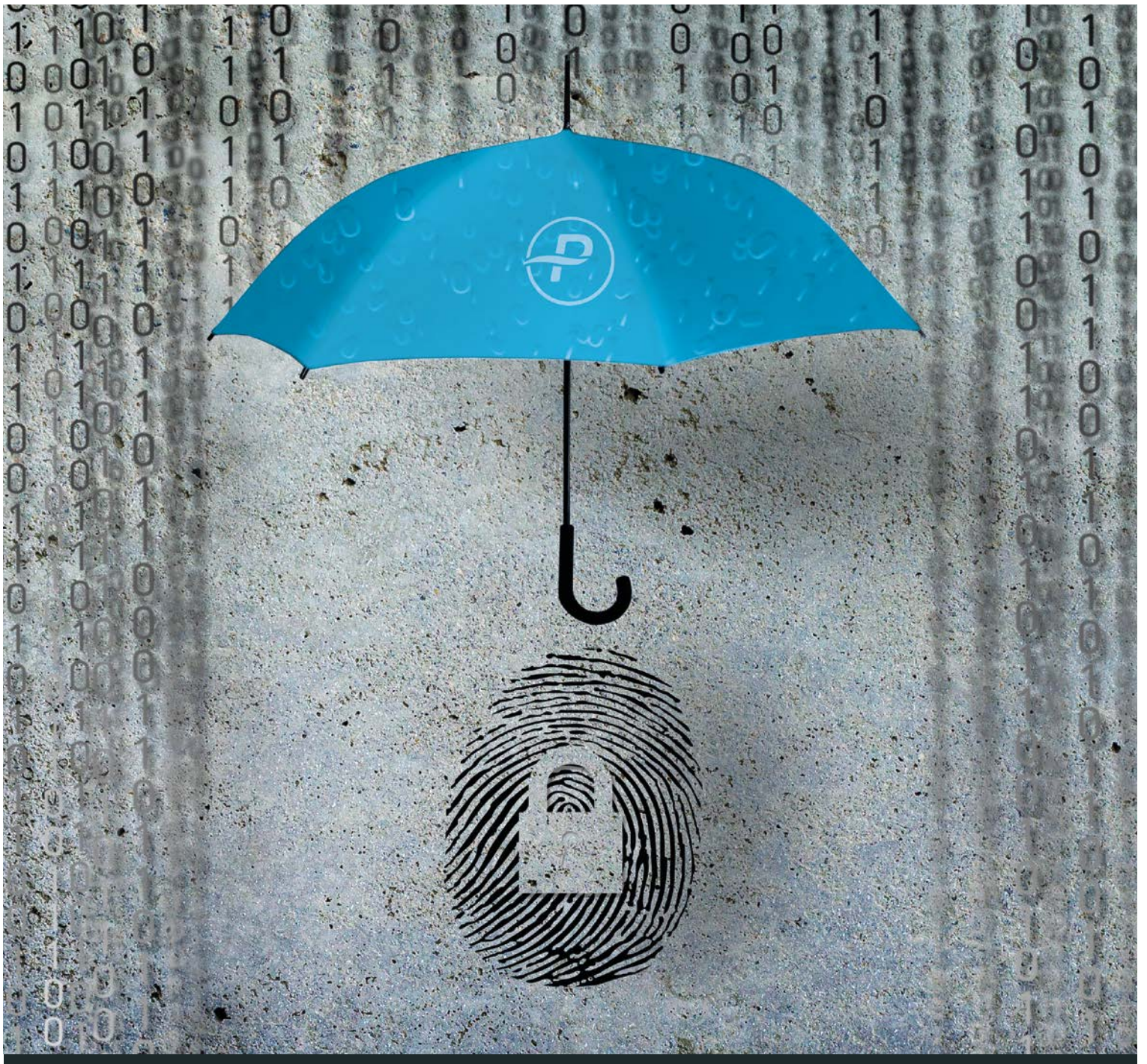


Einführung eines Datenschutz-Managementsystems

Wichtige Datenschutzinformationen

PROFLOW
Prozess- & Workflow-Management

Tim Iglauer,
ihr Datenschutzbeauftragter vor Ort

Liebe Leserin, lieber Leser,

mit der seit dem 25.05.2018 gültigen EU-Datenschutzgrundverordnung (EU-DSGVO) sind einige neue Vorgaben zu erfüllen.

Ziel der neuen EU-DSGVO ist es, ein einheitliches Schutzniveau für die Rechte und Freiheiten von natürlichen Personen bei der Verarbeitung von personenbezogenen Daten in allen europäischen Mitgliedstaaten zu gewährleisten - Ein Gesetz, welches für alle gültig ist!

Unter anderem wird von Unternehmen eine umfassende Nachweis- und Rechenschaftspflicht gefordert, sodass nicht nur die Sicherstellung der Datenschutzvorgaben nachzuweisen sind, sondern auch proaktiv die Angemessenheit des Datenschutzniveaus gewährleistet wird. **Durch die Rechenschaftspflicht wird die bisherige Lastenverteilung umgedreht und Sie müssen nun nachweisen, dass Ihr Datenschutz funktioniert** und das unabhängig davon, ob Schaden entstanden ist oder nicht.

Damit wird es unumgänglich, Prozesse umfangreich zu dokumentieren und eine Erfolgsmessung einzuführen. Nur so kann der Nachweis erfolgen, dass die Grundsätze der Datenverarbeitung nach EU-DSGVO eingehalten werden. Zudem ermöglicht ein solch effizientes Managementsystem schnellere Reaktionszeiten, falls es einmal zu einer Datenschutzpanne kommen sollte.

Eine unzureichende Dokumentation hinsichtlich des Datenschutzes kann sich hingegen bei der Festlegung eines möglichen Bußgeldes sehr negativ auswirken.

Somit ist die Einführung eines Datenschutz-Managementsystems (DSMS) nach EU-DSGVO für jedes Unternehmen sehr wichtig!

In dieser Ausgabe beschäftigen wir uns mit der Einführung und dem Betrieb eines Datenschutz-Managementsystems (DSMS) und Sie erhalten einen Überblick über bewährte Methoden und Hinweise zur konkreten Gestaltung eines DSMS.

Sollten Sie darüber hinaus weitere Informationen benötigen, stehen wir Ihnen jederzeit sehr gerne zur Verfügung. Sie erreichen uns unter der Telefonnummer **05665 / 180 98 50** oder per E-Mail an **tim.iglauer@proflow.de**.

Mit besten Grüßen

Tim Iglauer
B. Sc. Wirtschaftsinformatik
Externer Datenschutzbeauftragter

DSMS | Grundlagen zum Datenschutz-Managementsystem

Das Datenschutz-Managementsystem

Ein Datenschutz-Managementsystem (kurz: DSMS) stellt die Gesamtheit aller Dokumentationen, Regelungen, Maßnahmen und Prozesse dar. So werden die Anforderungen an die Verarbeitung personenbezogener Daten im Unternehmen gesteuert und kontrolliert. Man erhält ein Werkzeug, mit dem man durch kontinuierliche Planung, Umsetzung, Überwachung und Verbesserung eine einheitliche, strukturierte und nachhaltige Durchführung der Prozesse im Managementsystem sicherstellen kann.

Ziel des DSMS sollten nicht nur resultierende Maßnahmen zum Erreichen eines angemessenen Datenschutzniveaus sein, sondern eine koordinierte Vorgehensweise abbilden, um eine Risikolenkung zum Datenschutz entstehen zu lassen.

Ein Datenschutz-Managementsystem sollte grundsätzlich

- **auf bewährten Methoden zum Risikomanagement basieren (z.B. ISO 31000, IdW PS 340, etc.)**
- **Modular aufgebaut sein (verbindliche und optionale Komponenten beinhalten)**
- **eine Integration in eventuell vorhandene Qualitäts-Management-Systeme ermöglichen**

Risikomanagement

Risikomanagement wird grundsätzlich als ein fortlaufender Prozess verstanden, in dem Planung, Umsetzung, Überwachung und Verbesserung kontinuierlich stattfinden („Plan-Do-Check-Act“).

Modularer Aufbau

Um die hohen Anforderungen an die Dokumentation effizient und vollständig zu realisieren, sollten Module erstellt werden, welche die Struktur der Dokumentation und der gesetzlichen Vorgaben abbilden und individuelle Anforderungen der Unternehmen widerspiegeln. Sie können beispielsweise aus Dokumentvorlagen bestehen, um sie beliebig oft (und auch modulübergreifend) einsetzen zu können. Eine Anpassung und Erweiterbarkeit der Module und Vorlagen ist wünschenswert.

Integration in vorhandene Management-Systeme

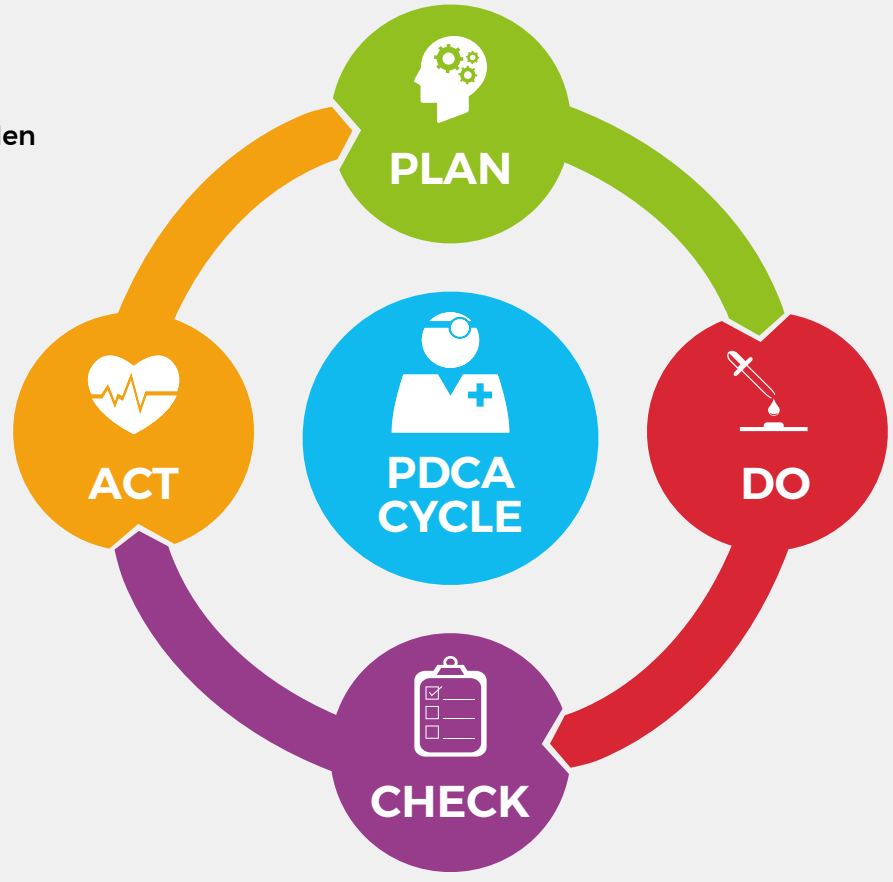
Existieren bereits Management-Systeme wie zum Beispiel zur Qualitätssicherung (ISO 9001) oder zur IT-Sicherheit (ISO 2700x oder IT-Grundschutz nach BSI), lassen sich doppelte Tätigkeiten vermeiden, weil bereits vorhandene Ressourcen genutzt und bestehende Management-Systeme erweitert werden können.

PLAN:
Die getroffenen technischen und organisatorischen Maßnahmen werden erst erdacht und geplant, ...

DO:
... im „kleinen Kreis“ getestet, ...

CHECK:
... die Wirksamkeit überprüft, ...

ACT:
... gegebenenfalls angepasst und dann im „Großen“ eingeführt.



DSMS | Ein Standardmodell

Standardmodelle

Die Einführung eines Datenschutz-Managementsystems ist vergleichbar mit der Implementierung eines Qualitäts-managementsystems (QMS).

Der schwierigste Schritt ist dabei meistens die Überführung der theoretischen Grund-lagenarbeit in die praktische Umsetzung. Angelehnt an diverse QMS-Standards kann das DSMS und dessen Implementierung in sechs Module unterteilt werden:

Datenschutzkultur

Um die Datenschutzziele zu erreichen, müssen die Geschäftsleitung und alle Führungskräfte ihre **Verpflichtung** zur Umsetzung des Datenschutzes deutlich formulieren und ihre Vorbildfunktion wahrnehmen, damit dem Datenschutzbeauftrag-ten (DSB) und der Datenschutzorganisation der Rücken gestärkt wird. In dieser Phase sollten sich Unternehmen folgenden Fragen stellen:

- **Was soll mit dem Datenschutz erreicht werden?**
- **Wie sehen die Vision zum Datenschutz aus?**
- **Was trägt der Datenschutz zu den Unternehmenszielen bei?**

1. **Datenschutzkultur**
2. **Datenschutzziele**
3. **Datenschutzrisiken**
4. **Datenschutzprogramm**
5. **Datenschutzorganisation/ -kommunikation**
6. **Datenschutzkontrolle**

1

Datenschutzziele

Zu den **Zielen** gehört es u. a. die Begriffe „Datenschutz“ und „Compliance“ inhaltlich in Bezug auf das Unternehmen zu definieren und i**n den Leitsätzen des Unternehmens zu verankern.** Die Ziele sollten dem Anspruch der Klarheit, Verständlichkeit und Messbarkeit genügen.

Dies ist ein sehr wichtiger Schritt, da er die Positionierung des Unternehmens zu diesem Thema verdeutlicht und zudem auch messbar macht. Dabei können bereits implementierte Grundsätze wie „verbindliche Unternehmens-richtlinien“ eine Basis darstellen.

Datenschutzrisiken

Effektiver Datenschutz kann nur implementiert werden, wenn ein risikobasierter Ansatz gewählt wird. Unternehmen sollten sich im Klaren darüber sein, welche Folgen z. B. der Verlust oder Missbrauch der personenbezogenen Daten für den Betroffenen und das Unternehmen haben kann. Risiken müssen dabei im Zusammenhang der Geschäftsfelder und des Informationswertes der zu verarbeitenden Daten gesehen werden.

Bekannte Probleme und die Komplexität des zu untersuchenden Datenverarbeitungsprozesses sind dabei zu berücksichtigen. Besonders bei der Verarbeitung von **sensiblen personenbezogene Daten** müssen **geeignete Schutzmaßnahmen** getroffen werden.

DSMS | Ein Standardmodell

Datenschutzprogramm

Hierbei handelt es sich um den größten Block bei der Implementierung eines Datenschutz-Managementsystems. In dieser Phase wird die Frage beantwortet, wie definierte Datenschutz-Anforderungen im Unternehmen umgesetzt werden. Folgende Arbeitspakete sind u. a. zu schnüren:

- **Erstellung von Richtlinien**
- **Regelung der Auftragsverarbeitung**
- **Umsetzung des Mitarbeiterdatenschutzes**
- **Umsetzung des Kundendatenschutzes**
- **Dokumentation der Verarbeitungstätigkeiten**
- **Erhebung und Bewertung der technischen und organisatorischen Maßnahmen**
- **Umsetzung der Betroffenenrechte**
- **Einführung eines Vorfall-Managements**

Datenschutzorganisation/ - kommunikation

In diesem Baustein wird beschrieben, wer die die definierten Datenschutz-Anforderungen im Unternehmen umsetzt.:

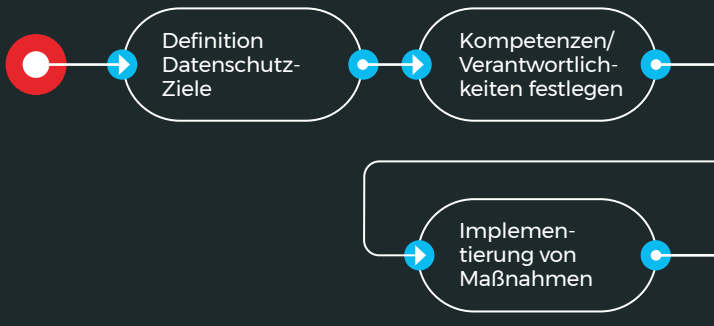
- **Rollen und Verantwortlichkeiten (z.B. Aufgaben des DSB)**
- **Leitlinien Datenschutz und Datensicherheit (z.B. Schutzziele)**
- **Ressourcenplanung (z.B. Budgetierung)**

Betroffene Mitarbeiter und ggf. Dritte werden in dieser Phase über das Datenschutz-Programm sowie über die Rollen und Verantwortlichkeiten informiert. Hier kann ein Berichtsweg für identifizierte Risiken, festgestellte Regelverstöße sowie eingehende Hinweise festgelegt werden. Zu den Aufgaben gehört:

- **Schulung der Mitarbeiter**
- **Festlegung der Kommunikation mit Externen**
- **Festlegung der internen Kommunikation (Awareness)**
- **Umgang mit Datenpannen**
- **Regelung von Anfragen und Beschwerden**
- **Implementierung des Reportings**

Prozessmodell zur Implementierung

Sind die verschiedenen Bausteine und Module definiert, muss der DSMS-Lifecycle im Unternehmen etabliert werden. Dabei ist es sinnvoll, die einzelnen Schritte (soweit wie möglich) zusammenzufassen und einem Prozessmodell zuzuordnen:



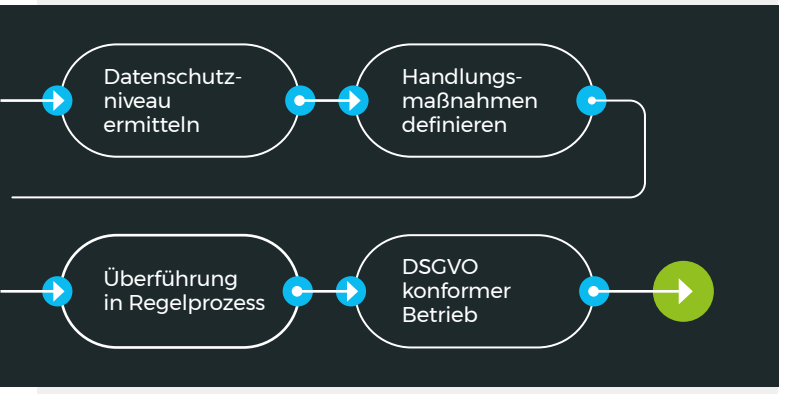
Datenschutzkontrolle

Zu guter Letzt muss das implementierte DSMS regelmäßig auf dessen Wirksamkeit geprüft werden. Dieses wird im Kontroll-Modul des Managementsystems definiert. Dazu gehören:

- **Implementierung ggf. von Datenschutz-folgenabschätzungen**
- **Jährliche Audits**
- **Kontinuierliche Verbesserungen (Stichwort: „PDCA-Zyklus“)**

Hinweis: QMS-Standards geben eine einheitliche Vorgehensweise vor, die sich auch gut auf den Datenschutz anwenden lässt. Die Umsetzung eines DSMS ist jedoch immer von unternehmerischen Entscheidungen abhängig. Eine unternehmensindividuelle Anpassung ist immer notwendig. Die hier aufgezeigten Module sind als mögliche Beispiele aufgeführt.

Wichtig: Unternehmen sollten sich frühzeitig mit dieser Thematik auseinander-setzen, da ein DSMS bei unbeabsichtigten Datenschutzverstößen nicht mit Sicherheit den Vorwurf der Fahrlässigkeit entfallen lässt, sich jedoch bußgeldmindernd auswirken kann. Entscheidender ist jedoch die schnelle Handlungsfähigkeit im Notfall oder bei Auskunftsersuchungen.



6

DSMS | IT-Sicherheitsrisiken minimieren

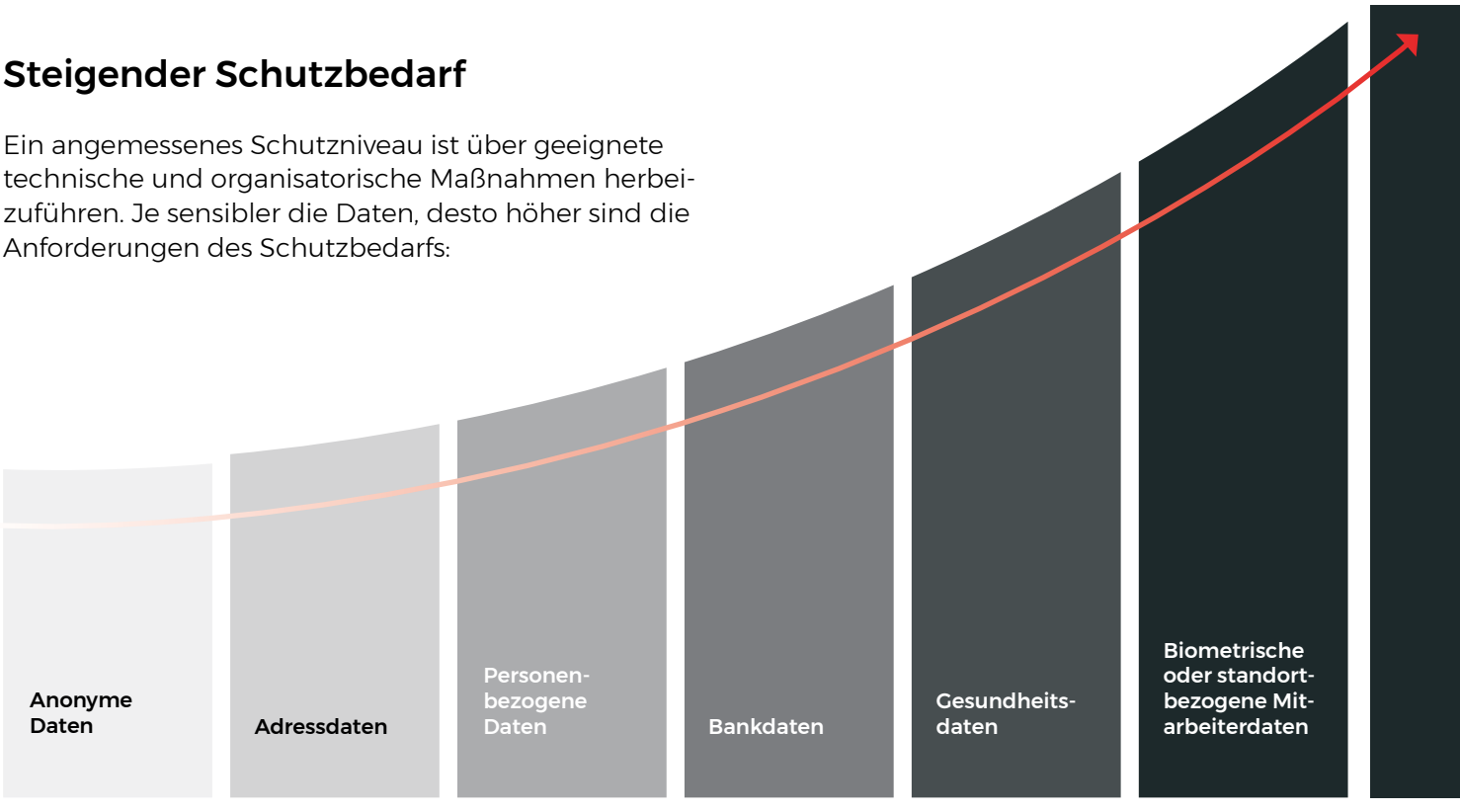
Minimierung von IT-Sicherheitsrisiken

Bei der Verarbeitung von personenbezogenen Daten ist gemäß Art. 32 Abs. 1b DSGVO die Einhaltung der drei IT-bezogenen Schutzziele (Verfügbarkeit, Vertraulichkeit und Integrität der Daten) sicherzustellen.

VERFÜGBARKEIT	**Handlungs-maßnahmen:**	**Reduzierung von:**
VERTRAULICHKEIT	**Prüfung der technischen und organisatorischen IT-Situation**	**Sicherheitsvorfällen und Angriffe durch Cyberkriminalität**
INTEGRITÄT	**Handlungsempfehlungen für IT-Sicherheitsmaßnahmen (BSI Grundschutz) erarbeiten**	**Verletzung der Rechenschaftspflicht** (Gem. Art. 5 Abs. 2 DSGVO ist die Einhaltung der Datensicherheit zu gewährleisten und nachzuweisen)

Steigender Schutzbedarf

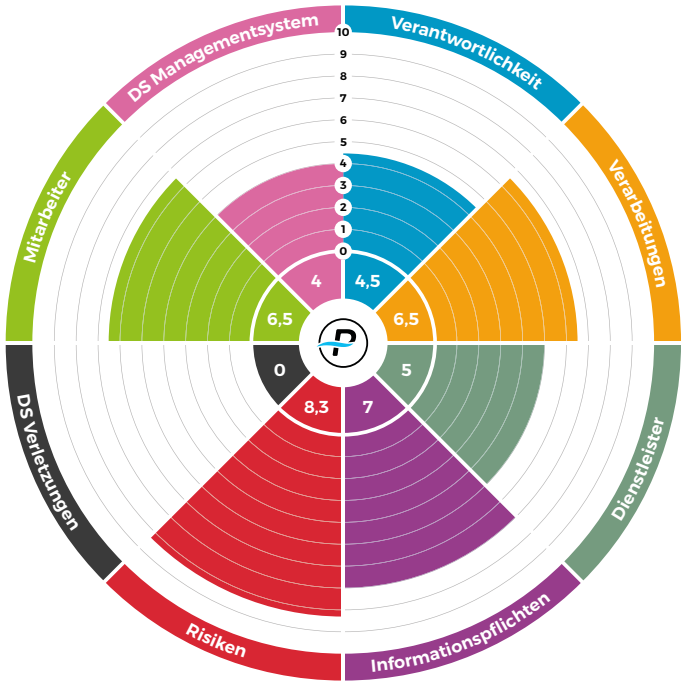
Ein angemessenes Schutzniveau ist über geeignete technische und organisatorische Maßnahmen herbeizuführen. Je sensibler die Daten, desto höher sind die Anforderungen des Schutzbedarfs:



DSMS | Fazit

Folgende Aufgaben ergeben sich für die Einführung eines DSMS:

- Definition „Datenschutz“ für das Unternehmen
- Leitlinie publizieren
- Verantwortlichkeiten festlegen
- Aktuelles Datenschutzniveau ermitteln (siehe Abbildung)
- Verarbeitungsverzeichnis erstellen
- Gesetzes- und Vorschriftsänderungen berücksichtigen
- Aufnahme der technischen und organisatorischen Begebenheiten
- Abgleich der Verfahren mit den gesetzlichen Anforderungen
- Ableitung von Handlungsempfehlungen nach SOLL/IST-Abgleich
- PDCA-Zyklus aktivieren
- Einführungs- und Kontrollprozess implementieren
- Sensibilisierung, Controlling, Reporting



Fazit

Für die Umsetzung der Datenschutzgrundverordnung (DSGVO) wird es nach wie vor keine Patentlösung geben. Jedes Unternehmen muss sich zwangsweise mit dem Thema auseinandersetzen, wobei die Einführung eines Datenschutz-Managementsystems (DSMS) Sie dabei unterstützt, der gesetzlich geforderten Nachweis- und Rechenschaftspflicht nachzukommen. Dabei soll das DSMS Sie jedoch nicht nur bei der Erfüllung der gesetzlichen Anforderungen unterstützen, sondern idealerweise Bußgelder vermeiden und schnelle Reaktionszeiten garantieren. Eine Kombination mit anderen Managementsystemen ist durchaus möglich, so dass doppelte Tätigkeiten vermieden werden können.

Sprechen Sie mich gerne an und profitieren Sie von meinen Erfahrungen bei der Einführung von Datenschutz-Management-Systemen.

Ihr Tim Iglauer

Tim Iglauer
B. Sc. Wirtschaftsinformatik
Externer Datenschutzbeauftragter

PROFLOW
Prozess- & Workflow-Management

Unter den Pappeln Str. 7
34327 Körle

Tel.: 05665 / 180 98 50
Fax: 05665 / 180 98 51
E-Mail: tim.iglauer@proflow.de

www.proflow.de