Kurz und knapp erklärt:

Technische und organisatorische Maßnahmen

[Anforderung] Was sagt das Gesetz?

Die konkret geforderten Maßnahmen nach Art. 32 DSGVO, werden im Gesetzestext nicht näher beschrieben, sondern abstrahiert dargestellt.

> ***Artikel 32:***
>
> *„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 […] geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; […]“*

[Maßnahmen] Was ist zu tun?

Um nun konkret bestimmen zu können, welche Maßnahmen zu treffen sind, müssen folgende Schritte gesetzt werden:

» Durchführung einer Risikoabschätzung der Datenverarbeitungen (siehe One Pager „Risikobewertung“)

» Festlegung geeigneter Maßnahmen zur Risikoverminderung;

» Regelmäßige Evaluierung der Angemessenheit/Geeignetheit der Maßnahmen;

Hinweis: Werden Auftragsverarbeiter eingesetzt, so sind auch deren technische und organisatorische Maßnahmen regelmäßig zu kontrollieren (siehe One Pager „Outsourcing“).

[Nutzen] Was bringt mir das?

Die Implementierungen geeigneter Schutzstandards bietet viele umfangreiche Vorteile:

» Erhöhung des Schutzniveaus bei Vertraulichkeit, Verfügbarkeit und Integrität

» Reduzierung von Datenpannen und Sicherheitsvorfällen

» Budget-Optimierung in der IT, da keine „überzogenen“ (in der Regel kostspieligen) Sicherheitsmaßnahmen ergriffen werden

» Erhöhung der Akzeptanz von Sicherheitsmaßnahmen bei den Usern durch Angemessenheit

» Positive Auswirkungen auf das Business Continuity

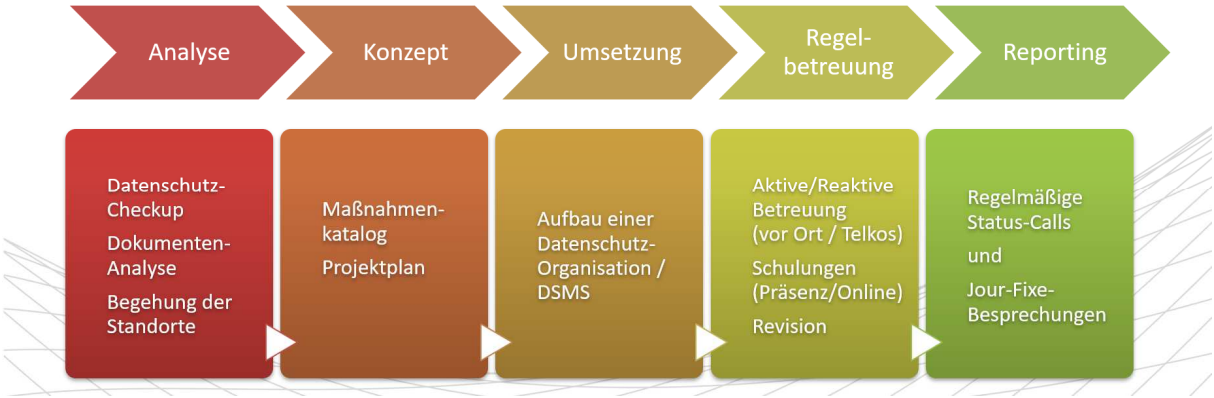
[UIMC] Wie hilft die UIMC?

Die UIMC hat Templates für ein Informationssicherheits- und Datenschutzhandbuch und bietet Tools für die Durchführung von effizienten Audits, Revisionen und Risikobewertungen. Hierbei kommen Berater mit langjähriger Erfahrung und umfassender Fach-Expertise und Methoden-Know-How zum Einsatz.

[Anlage] Datenschutz-Managementsystem

Das prinzipielle Vorgehen der UIMC in der Beratung zeichnet sich durch eine Mischung aus vorstrukturierten und standardisierten Verfahrensweisen mit unterstützenden Hilfsmitteln sowie individuellen Problemlösungen aus. Hierbei hat sich ein top-down-orientiertes Vorgehensmodell bewährt, das in Anlehnung an gängige Standards erarbeitet worden ist.

Nach erfolgter Analyse wird in Form eines Maßnahmenkatalogs ein Umsetzungskonzept erarbeitet und eine Datenschutz-Organisation bzw. ein Datenschutz-Managementsystem aufgebaut. In Form der Regelbetreuung werden neben einer Projektverfolgung Adhoc-Anfragen bearbeitet, regelmäßige Abstimmungen und Revisionen vorgenommen sowie eine Umsetzung vorangetrieben (inkl. Schulungen). Auch findet ein regelmäßiges Reporting inkl. eines jährlichen Tätigkeitsberichts an die Geschäftsführung statt.



Erfahrungsgemäß ist davon auszugehen, dass für den Aufbau einer Datenschutz-Organisation im Rahmen des Initialprojekts ca. 2 Jahre ab Betreuungsstart benötigt werden. Dies ist auch abhängig von den Ergebnissen der Analysephase sowie den internen und externen Ressourcen für die Datenschutz-Tätigkeiten.