Datenschutz: Das APP 360°-Modell

Veröffentlicht am 7. Februar 2019

Ihre Ansprechpersonen: Stefan P. Hauser

Tags: Fachbeiträge, Ausschreibung und Evaluation, Business Analyse und Requirements Engineering, Projektmanagement, Prozessoptimierung und -management, Schulung und Training, Strategieberatung

DSGVO - Hintergrund und Konsequenzen

Am 25. Mai 2018 trat die EU-Datenschutzgrundverordnung (DSGVO) in Kraft, welche von Unternehmen mehr Verantwortung bezüglich Schutz von personenbezogenen Daten fordert. Auch das Schweizerische Datenschutzgesetz (DSG) wird aktuell revidiert.

Zur «Verbesserung der Transparenz von Datenbearbeitungen» und zur «Stärkung der Selbstbestimmung betroffener Personen über ihre Daten», hat der Bundesrat am 15. Dezember 2017 die Botschaft zur Totalrevision des Datenschutzgesetzes verabschiedet. Gepaart mit der geplanten Anpassung des DSG, verschärft die DSGVO die Pflichten von Unternehmen und fordert diese auf, Strukturen und Prozesse anzupassen.

Die Umsetzung der neuen Datenschutzvorschriften ist für grosse wie kleine Unternehmen ein Projekt mit grosser Tragweite, welches ein strukturiertes Vorgehen erfordert.

Dieser Fachbeitrag adressiert Herausforderungen und Chancen der Vorgabenumsetzung, definiert Massnahmen zur Sicherstellung der Compliance und skizziert einen Leitfaden zur Umsetzung der neuen Vorgaben.

Datenschutz – Herausforderungen und Opportunitäten

Die DSGVO beinhaltet Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Art. 1 Abs. 2 DSGVO).

Personenbezogene Daten umfassen dabei alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen (Art. 4 Abs. 1 DSGVO). Die Verarbeitung beinhaltet alle Vorgänge in Zusammenhang mit personenbezogenen Daten (Art. 4 Abs. 2 DSGVO). Dies betrifft nicht nur die Erhebung, sondern auch die Speicherung, die Analyse, die Übermittlung oder gar das Löschen von Daten.

Anwendung findet das DSGVO auch bei einem Grossteil der Schweizer Unternehmen, zum Beispiel wenn diese Waren oder Dienstleistungen an Personen mit Aufenthalt in der EU anbieten, deren Verhalten beobachten oder diese über eine EU-Niederlassung verfügen (Art. 3 Abs. 2 DSGVO).

Folgende Vorgaben können für Schweizer Unternehmen zu Herausforderungen führen:

Rechenschaftspflicht Art. 5 Abs. 2 DSGVO

Die DSGVO beinhaltet eine Beweislastumkehr und fordert von Unternehmen umfassende Dokumentations- und Nachweispflichten der Datenschutz-Compliance. Die Erstellung und Pflege dieser Dokumentation ist häufig zeit- und kostenintensiv.

Privacy by design and by default Art. 25 DSGVO

Gemäss der DSGVO sind Datenschutzgrundsätze auch mittels technischer und organisatorischer Massnahmen zu implementieren, beispielsweise durch datenschutzfreundliche Werkeinstellungen. Das Gebot nach Datenschutz durch Technikgestaltung kann für Unternehmen somit technische und organisatorische Anpassungen von Dienstleistungen und Produkten zur Folge haben.

Verzeichnis von Verarbeitungstätigkeiten Art. 30 Abs. 1 DSGVO

Gemäss der DSGVO ist ein Verzeichnis der Verarbeitungstätigkeit zu erstellen. Dieses dient als Übersicht darüber, welche Daten wie und zu welchem Zweck verarbeitet werden. Das Verarbeitungsverzeichnis ist ein wesentlicher Bestandteil der Dokumentationspflicht. Oft werden Personendaten jedoch in verschiedenen

Geschäftsprozessen verarbeitet und auf unterschiedlichen Systemen und Medien gespeichert, ohne dass dies dokumentiert wird. Die Schaffung vollständiger Transparenz über die Datenverarbeitung ist eine herausfordernde und komplexe Aufgabe, welche entsprechende Ressourcen verlangt.

Datenschutz-Folgeabklärung Art. 35 DSGVO

Ist eine Datenverarbeitung für eine Person voraussichtlich mit einem hohen Risiko für die Rechte und Freiheiten behaftet, so ist eine Datenschutz-Folgenabschätzung vorzunehmen. Für die Durchführung der Datenschutz-Folgeabklärung sowie für die ordnungsgemässe Dokumentation sind entsprechende Prozesse zu entwerfen und einzuführen. (1)

Betroffenenrechte Art. 12-23 DSGVO

Die DSGVO beinhaltet wesentliche Rechte für Betroffene, wie beispielsweise die Informationspflicht bei der Erhebung personenbezogener Daten (Art. 13 DSGVO), das Recht auf Berichtigung (Art. 16 DSGVO) oder das Recht auf Löschung (Art. 17 DSGVO). Für die Umsetzung der Betroffenenrechte und deren Dokumentation sind Strukturen und Prozesse einzuführen, welche strukturelle und organisatorische Anpassungen zur Folge haben.

Melde- und Informationspflicht Art. 33-34 DSGVO

Kommt es zu einer Verletzung des Schutzes personenbezogener Daten, so sind die Aufsichtsbehörde und die betroffene Person zu benachrichtigen. Zur Erkennung von Datenschutzverletzungen und zum ordnungsgemässen Umgang mit Melde- und Informationspflichten sind entsprechende Strukturen und Prozesse zu implementieren. Das Erkennen von Datenschutzverletzungen bedingt vollständige Transparenz über die bestehenden Datenverarbeitungen.

Die Operationalisierung neuer Vorgaben zum Datenschutz hat nicht nur strukturelle und organisatorische Anpassungen zur Folge, sondern ist je nach Unternehmen auch ein komplexes, langwieriges und teures Unterfangen. Auf der anderen Seite birgt die Operationalisierung neuer Vorgaben auch wesentliches Synergiepotential. So bietet beispielsweise die Notwendigkeit der umfassenden Betrachtung der Verarbeitungstätigkeit die Möglichkeit, dass Prozesse und Strukturen gesamtheitlich analysiert und Ineffizienzen erkannt werden.

Innerhalb eines Datenschutzprojekts geht es somit nicht nur um die Umsetzung von Vorgaben, sondern auch um eine optimal auf Kundenbedürfnisse, Infrastruktur und Ressourcen abgestimmte Prozessgestaltung, was wiederum zum wirtschaftlichen Erfolg beiträgt.

Compliance – Strategien und Massnahmen

Die Implementierung neuer Datenschutzvorschriften kann im Rahmen eines vollumfänglichen Projekts oder durch die Umsetzung einzelner Massnahmen erfolgen.

Zur Sicherstellung der Compliance müssen aber mindestens die folgenden Schritte vorgenommen werden:

Datenschutzerklärung

Gemäss der DSGVO müssen betroffene Personen über die Erhebung ihrer personenbezogenen Daten informiert werden (Art. 1 DSGVO). Dies erfolgt in der Regel in Form einer Datenschutzerklärung, die erstellt und sichtbar auf der Website publiziert wird.

Verzeichnis der Verarbeitungstätigkeit

Zur Erfüllung der Dokumentationspflichten ist ein Verarbeitungsverzeichnis zu erstellen, das die gesetzlich verlangten Angaben beinhalten muss (Art. 30 DSGVO). Sind die Verarbeitungstätigkeiten nicht dokumentiert, kann diese Massnahme zu einem komplexen und umfassenden Unterfangen werden.

Vertragsprüfung und -anpassung

Gemäss dem Schweizerischen Datenschutzgesetz (DSG) darf die Bearbeitung von Personendaten an Auftragnehmer (Outsourcing) übertragen werden (Art. 10a DSG). Der Auftraggeber hat dabei sicherzustellen, dass der Auftragnehmer bei der Datenverarbeitung jene Datenschutzvorgaben einhält, denen der Auftraggeber unterliegt. Ändert sich für den Auftraggeber die gesetzliche Grundlage, so sind die Verträge mit Auftraggebern dahingehend zu prüfen, ob diese mit den neuen Vorgaben übereinstimmen. Gegebenenfalls sind Anpassungen vorzunehmen.

Prozessgestaltung

Zur Sicherstellung der Betroffenenrechte sowie der Melde- und Informationspflichten sind Prozesse einzurichten.

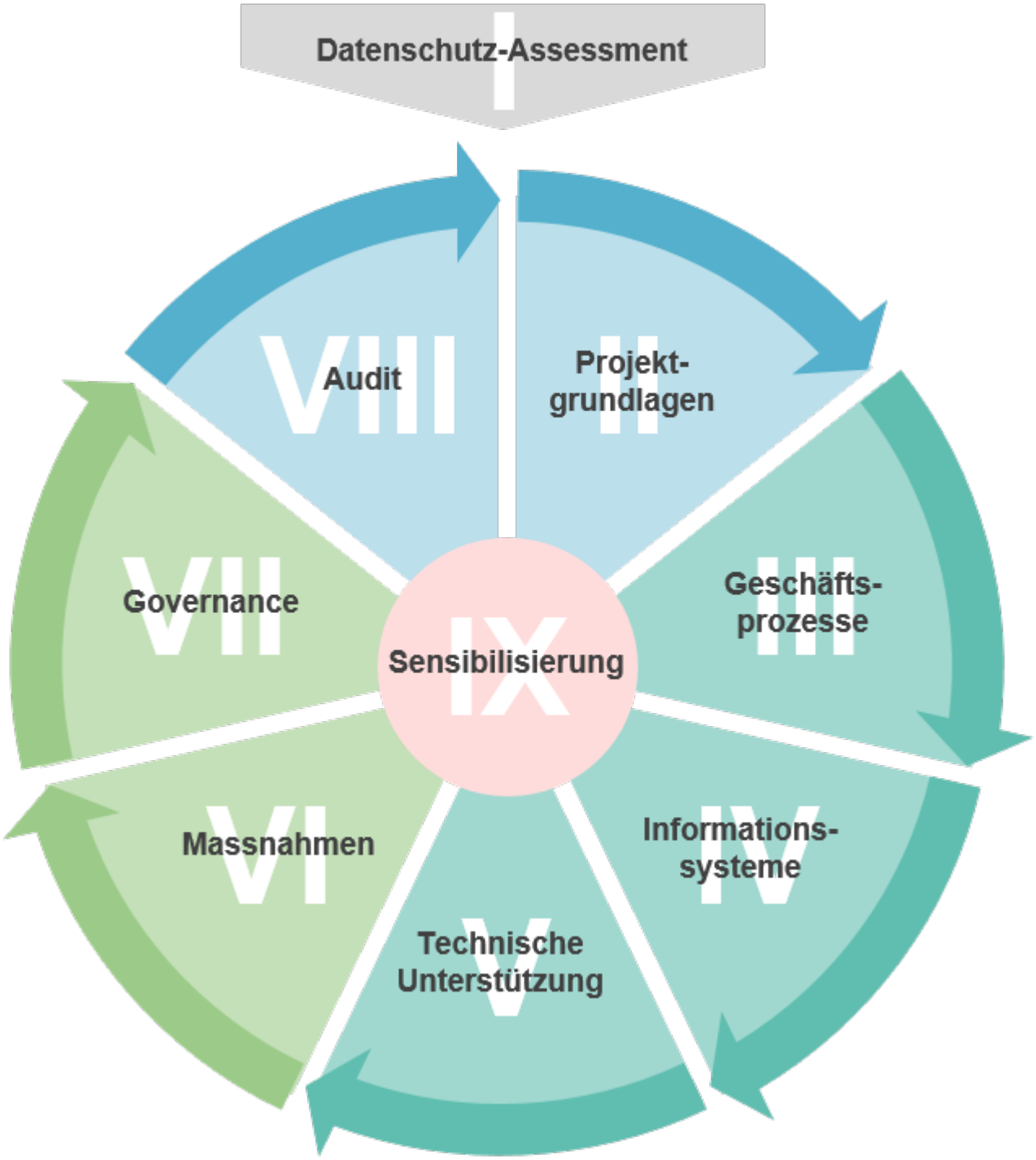
Die Umsetzung punktueller Massnahmen ist zwar effektiv im Sinne der Gewährleistung der Compliance, jedoch nicht effizient. Die Umsetzung einzelner Massnahmen führt dazu, dass diese nicht aufeinander abgestimmt sind und bei Änderungen in Struktur und Organisation erneut durchlaufen werden müssen. Ebenfalls besteht in der Umsetzung punktueller Massnahmen nur geringe Synergie.

Zur Schaffung und Nutzung des Synergiepotentials innerhalb der Implementierung von Datenschutzvorschriften ist ein gesamtheitlicher Ansatz nötig. Einen solchen stellen wir Ihnen mit unserem 360°-Modell vor.

360°-Modell - Leitfaden und Umsetzung

Die Operationalisierung von Datenschutzvorgaben bedarf einer sorgfältigen Planung (2). Das APP 360°-Modell dient als Leitfaden zur Operationalisierung von Datenschutzvorschriften.

Inspiriert vom Modell der Unternehmensarchitektur (3) gehen wir von einem gesamtheitlichen Ansatz aus, welcher die Operationalisierung von Datenschutzvorgaben als iterativen und kontinuierlichen Prozess betrachtet.



Mit dem Modell werden drei konkrete Ziele verfolgt:

- Sicherstellung der Datenschutz-Compliance
- Schaffung von Transparenz in Strukturen und Prozessen

- Kontinuierliche Überprüfung und nachhaltige Etablierung von Datenschutz innerhalb der Organisation

Ausgehend von einem Datenschutz-Assessment führt das Modell strukturiert durch definierte Elemente. Das Modell ist als Kreislauf aufgebaut, wodurch die Modellelemente nach Bedarf und Notwendigkeit wiederholt werden. Die Tabelle auf der nächsten Seite erläutert die Inhalte der Modellelemente.

Datenschutz Assessment

AuditMit dem Datenschutz-Assessment wird der Handlungsbedarf bezüglich Daten-schutz geprüft. Verarbeitet ein Unternehmen gar keine personenbezogenen Daten, besteht auch kein Handlungsbedarf zum Datenschutz. Werden personenbezogene Daten verarbeitet, empfiehlt sich eine Anwendung des 360°-Modells.

Projektgrundlagen

Die Operationalisierung von Datenschutzvorschriften innerhalb eines Unterneh-mens wird als Umsetzungsprojekt geplant. Entsprechend werden Projektgrund-lagen geschaffen. Diese umfassen das Festlegen von Projektteam, Projektzie-len, Projektplanung, Projektbudget sowie Projektressourcen. Ebenfalls wird eine Rechtsgrundlagenanalyse erstellt, in welcher die relevanten gesetzlichen Vorga-ben und deren Anwendung für die Organisation dokumentiert werden. In der Risi-koanalyse werden relevante Risiken aufgenommen.

Geschäftsprozesse

Die Geschäftsprozesse werden hinsichtlich der Verarbeitung personenbezogener Daten untersucht und der IST-Zustand dokumentiert. Auf Basis der zuvor festge-legten Ziele und rechtlichen Vorgaben wird der SOLL-Zustand definiert. Aus dem Vergleich zwischen IST- und SOLL-Zustand wird der Anpassungsbedarf festgelegt.

Informationssysteme

Die Informationssysteme, bestehend aus Applikationen und Daten, werden hin-sichtlich der Verarbeitung personenbezogener Daten untersucht und der IST-Zu-stand der Daten- und Applikationsarchitektur dokumentiert. Auf Basis der Pro-jektziele und rechtlichen Vorgaben (insb. Privacy by design and default) wird der SOLL-Zustand definiert. Der Anpassungsbedarf bei den Informationssystemen wird dokumentiert.

Technische Infrastruktur

Die Elemente der technischen Infrastruktur, welche für den Aufbau und den Be-trieb der Informationssysteme notwendig sind, werden hinsichtlich der Verarbei-tung personenbezogener Daten untersucht und der IST-Zustand dokumentiert. Auf Basis der Projektziele und der rechtlichen Vorgaben (insb. Privacy by design and default) wird der SOLL-Zustand definiert. Der Anpassungsbedarf zu der technischen Infrastruktur wird dokumentiert.

Massnahmen

Basierend auf den Erkenntnissen und Resultaten aus den Elementen II-V wird ein konsolidierter und priorisierter Massnahmenkatalog erstellt.

Governance

Die Governance beinhaltet die Umsetzung der definierten Massnahmen als auch die Prüfung und Sicherstellung der geforderten Dokumentationspflicht.

Audit

Das Audit beinhaltet die regelmässige Überprüfung der Datenschutzmassnahmen und der Einhaltung von rechtlichen Vorgaben. Änderungen rechtlicher Vorgaben oder strukturelle Anpassungen werden dahingehend beurteilt, ob das 360°-Modell erneut durchlaufen werden muss.

Personen

Das zentrale Element eines jeden Umsetzungsprojektes zum Datenschutz ist das Management der Personenkreise, welche an der Datenverarbeitung direkt oder auch indirekt beteiligt sind. Nichtwissen, Überforderung, Leichtsinn oder Vorsatz kann dazu führen, dass definierte Massnahmen zum Schutz von personenbezoge-nen Daten nicht oder mangelhaft umgesetzt werden. Aus diesen Gründen ist es wichtig, Mitarbeitende, Lieferanten und Partner aktiv in das Datenschutzprojekt einzubeziehen und Massnahmen zur Kommunikation und Ausbildung sowie Hilfe-stellung zu definieren.

(1) Wybitul, T., Breunig, C. & Ströbel, L. (2017). Praktische Hinweise zur DSGVO-Umsetzung. Zeitschrift für Datenrecht und Informationssicherheit digma. (17. Jahrgang, Heft 1), S. 23-24.

(2) Wybitul, T., Breunig, C. & Ströbel, L. (2017). Praktische Hinweise zur DSGVO-Umsetzung. Zeitschrift für Datenrecht und Informationssicherheit digma. (17. Jahrgang, Heft 1), S. 20-21.

(3) Eine Unternehmensarchitektur beschreibt die ganzheitliche Sicht auf die Geschäfts- und IT-Strukturen, wobei die Unternehmensarchitektur das Zusammenspiel der drei Sichten Geschäftsarchitektur, Informationssystemarchitektur und Technologiearchitektur illustriert.