Datenschutz
Einfach
Digital
Gestalten

An der Startlinie zur Umsetzung
Ein strategischer Fahrplan

DS-GVO

2018

Der Begriff „DS-GVO“ geistert nun zunehmend durch den Alltag von Unternehmen. Fast schon bedrohlich lesen sich Artikel und Stellungnahmen in der Presse und in den neuen Medien. Meist ist die Rede von einem hohen Aufwand, von hohen Kosten und kaum ausreichend Zeit, alle Anforderungen zielgerecht umzusetzen. Dabei wirft die IT-Sicherheit ihre Schatten voraus. Sie ist fast schon zu einem Synonym zur DS-GVO geworden. Kaum noch ist ein Dienstleister oder Lösungsanbieter von IT- und Softwaresystemen auf dem Markt zu finden, bei dem Begrifflichkeiten aus dem Datenschutz fehlen. Das ist nicht verwunderlich, wonach digitale Anwendungen und arbeitsteilige Prozesse, auch mit Dienstleistern, deutlich erhöhte Anforderungen an ein Unternehmen stellen. Allerdings umfasst die DS-GVO noch weitere zahlreiche Gesichtspunkte, die ebenfalls berücksichtigt und vor allem umgesetzt werden müssen. Ein komplexes Thema, was einfach gestaltet werden muss.

Viel Erfolg wünscht Ihnen

Marc Weber

Schritt 1: Aktuelle Situation

In einem ersten Schritt ist es zunächst unerlässlich, sich einen Überblick im eigenen Unternehmen zu verschaffen. Dabei liegt der Kern des Fokus eindeutig auf den Prozessen und Arbeitsabläufen, die auf personenbezogenen Daten beruhen oder mit diesen umgehen. In diesem Schritt lässt sich zudem feststellen, ob Datenbestände an personenbezogenen Daten vorhanden sind, die nicht aktiv benötigt werden.

Für eine aktuelle Ist-Analyse sollte u.a. geprüft werden:

- **Verfahren** – identifizieren Sie aktuelle Arbeitsabläufe und Prozesse, die in Verbindung mit personenbezogenen Daten stehen. Optimal hierzu ist ein aktuelles Verfahrensverzeichnis.

- **Grundlage** – stellen Sie sich die Frage, ob die aktuell vorhandenen oder geplanten personenbezogenen Daten verarbeitet / erhoben werden dürfen. Ist eine Einwilligung vorhanden oder erlaubt eine Rechtsvorschrift den Umgang.

- **Mitarbeiter** – insbesondere Angestellte, die mit personenbezogenen Daten arbeiten sind auf das Datengeheimnis zu verpflichten und entsprechend den Anforderungen zu schulen.

- **Dienstleister** – der Einsatz externer Dienstleister ist vielfältig und kann nahezu alle Disziplin in einem Arbeitsprozess erfassen. Prüfen Sie die Vertragsgrundlagen im Hinblick auf die Datenschutzanforderungen.

- Arbeiten Sie selbst als Dienstleister mit personenbezogenen Daten Ihrer Kunden, so überprüfen Sie die Umsetzung der Anforderungen Ihrer Kunden.

- **Organisation** – ein umfassendes betriebliches Datenschutzmanagement ist bei einem Umgang mit personenbezogenen Daten unerlässlich. Insbesondere sind die getroffenen technisch organisatorischen Maßnahmen zum Schutz der Daten zu prüfen.

- **Dokumentation** – eine nachvollziehbare Organisation lebt von der Dokumentation, anhand derer Maßnahmen und deren Umsetzung nachvollzogen werden können. Fehlende Nachweise werden i.d.R. mit „nicht umgesetzt“ bewertet.

- **Technik** – in digitalen Zeiten spielt die Technik eine bedeutende Rolle. Die eingesetzten Lösungen müssen dem Stand der Technik sowie dem Schutzbedarf der Datenbestände entsprechen.

Schritt 2: Konformitätsabgleich

Auf der Grundlage des festgestellten Ist-Zustandes lässt sich ein Konformitätsabgleich mit dem künftigen Soll-Zustand der DS-GVO erarbeiten. (Sie können auch den Ist-Zustand parallel mit dem Soll-Zustand der aktuellen BDSG vergleichen. Auftretende Abweichungen können hierdurch noch behoben werden.)

Bedeutende Kriterien sind u.a.:

- **Datenbestand** – Arten der Daten und deren Grundlage für eine Verarbeitung (bspw. Einwilligung oder gesetzliche Grundlage)
- **Mitarbeiter** – vertragliche Vereinbarungen sowie Schulungen und Unterweisungen
- **Dienstleister** – konkrete Tätigkeit festlegen und ein Umgang mit personenbezogenen Daten nur mit entsprechender Vereinbarung
- **Organisation** – neue Anforderungen an die technisch organisatorischen Maßnahmen zum Schutz der Daten
- **Dokumentation** – umfangreichere Auskunft über Entscheidungen und Handlungen mit Bewertungen und Risikoanalysen
- **Technik** – veränderten Stand der Technik, sowie erhöhte Anforderungen berücksichtigen

Schritt 3: Handlungsbedarf ermitteln

Sind bei dem Soll-Ist-Abgleich Lücken aufgetreten, so ergibt sich hieraus der nachfolgende Handlungsbedarf. Gehen Sie wertungsfrei mit den festgestellten Defiziten um, insbesondere mit Themen, die sich aus der Neuordnung der DS-GVO ergeben und bisher nicht gefordert oder relevant gewesen waren und listen Sie diese gesondert auf. Idealerweise wird der zu überarbeitende Gesichtspunkt eindeutig und verständlich formuliert und Abhängigkeiten innerhalb der Datenschutzorganisation skizziert. Auf diese Weise erhalten Sie einen ersten Eindruck über den Umfang und die erforderlichen Maßnahmen zur Umsetzung der geforderten Maßnahmen. Gehen Sie in Schritt 1 und 2 gezielt auf die besonderen Umstände Ihres Betriebes, der Mitarbeiterstruktur und der Waren / Dienstleistungen ein.

- **Ist-Abgleich** – Sie haben Ihre Organisation überprüft und wissen, welche Prozesse mit welchen personenbezogenen Daten existieren und welche technisch organisatorischen Maßnahmen dahinter stehen.

- **Soll-Abgleich** – Sie haben sich mit den Neuerungen und den Anforderungen der DS-GVO beschäftigt und können die Auswirkungen auf Ihr Unternehmen einschätzen.

- **Soll-Ist-Analyse** – Sie haben Ihren derzeitigen Ist-Zustand mit dem zukünftigen Soll-Zustand verglichen und konnten dabei den Handlungsbedarf ermitteln.

- **Übersicht** – aus dem festgestellten Handlungsbedarf ergibt sich eine Übersicht anstehender Tätigkeiten, die bis zum Stichtag umzusetzen sind.

Schritt 4: Aktionsplan

Betrachten Sie die einzelnen Defizite und bewerten Sie diese nach Dringlichkeit und eventuell benötigtem Ressourceneinsatz (finanzielle Mittel, Zeit, eventuell externe Unterstützung). Vergeben Sie den anstehenden Tätigkeiten dabei eine auf Ihre individuelle Situation ausgerichtet Hierarchie. Berücksichtigen Sie in jedem Fall den zeitlichen Faktor der geplanten Tätigkeiten um nicht in Verzug zu geraten. Oftmals wird dieser sehr knapp bemessen und in der späteren Praxis nicht eingehalten. Bedenken Sie auch eventuell anfallende Neuanschaffungen im Bereich von Datenverarbeitungsanlagen (Software, Hardware, Applikationen) um den Grundsätzen „Datenschutz durch Technik“ und „Datenschutz durch Voreinstellung“ gerecht zu werden.

- **Prioritäten festlegen** – ordnen Sie die anstehenden Tätigkeiten nach Dringlichkeit und Tragweite. (Haben Sie zudem einen Abgleich mit dem aktuellen Soll durch das BDSG durchgeführt, können gewonnene Erkenntnisse ebenfalls in die Priorisierung einfließen.)

- **Zeitplan** – berücksichtigen Sie neben den Prioritäten auch die abgeschätzte Zeit für die Umsetzung einzelner Tätigkeiten und stellen einen Zeitplan auf. Planen Sie vorsorglich stets ein erweitertes Zeitkontingent für jede Tätigkeit ein.

- **Ressourcen** – die Umsetzung wird auch ein gewisses Budget direkt durch Ausgaben für bspw. neue Software oder Schulungen aber auch indirekt durch Bindung von Arbeitsleitung eigener Mitarbeiter in Anspruch nehmen. Berücksichtigen Sie dies bei Ihren Planungen.

- **Technik** – die DS-GVO stützt sich in erster Linie auf Technik und Technologie. Eingesetzte automatisierte Systeme sind hohen Ansprüchen ausgesetzt. In der Praxis kann dies zu Neuanschaffungen führen.

- **Externe Hilfe** – planen Sie bei Bedarf frühzeitig externe Hilfe bspw. für den Bereich IT und IT-Sicherheit ein.

Schritt 5: Umsetzung + Betrieb

Gehen Sie die einzelnen Organisationsschritte entsprechend Ihrer Planung zur Umsetzung an. Bei Bedarf können Sie sich Rat in Fachliteratur, Seminaren oder durch externe Berater einholen. Auch die zuständigen Aufsichtsbehörden bieten i.d.R. kostenfreie Ratgeber und Praxishilfen und stehen, je nach Personalstruktur, bei Fragen zur Umsetzung mit Rat und aktuellen Auslegungsansichten zur Seite. Behalten sie auch während der Umsetzungsphase die aktuelle Entwicklung im Auge, um bei Bedarf rechtzeitig auf veränderte Ausgangslagen reagieren zu können. Haben Sie bis zu dem Stichtag 25.05.2018 Ihre Datenschutzorganisation reorganisiert und auf die Anforderungen durch die DS-GVO optimiert, so ist empfehlenswert die aktuelle Situation weiterhin im Blick zu behalten. Aktuelle Auslegungsentscheidungen und gerichtliche Urteile können eine Anpassungsgrundlage Ihrer Organisation begründen.

- **Start** – beginnen Sie mit der Umsetzung der beschriebenen Tätigkeiten und Maßnahmen entsprechend Ihrem aufgestellten Zeitplan.

- **Unklarheit** – zahlreiche Ratgeber, Fachliteratur, Vorträge oder Seminare bieten gezielte und zum Teil kostenfreie Informationen über die DS-GVO und deren praktische Umsetzung. Nutzen Sie diese Möglichkeiten, sobald es in der Realisierungsphase zu Problemen kommt.

- **Aktualität** – behalten Sie aktuelle Entwicklungen im Auge und passen Sie frühzeitig Ihre Arbeiten den geänderten Einschätzungen an.

- **Stichtag** – haben Sie es geschafft, Ihre Organisation bis zu dem Stichtag umzusetzen, ist ein bedeutender Meilenstein geschafft. Bleiben Sie jedoch stets aufmerksam, um Veränderungen und Neuerungen frühzeitig einplanen zu können.

Anhang

Bei der Ein- und Abschätzung der anstehenden Anforderungen durch die DS-GVO sind insbesondere, jedoch nicht abschließend, die Artikel:

5 Grundsätze für die Verarbeitung personenbezogener Daten
7 Bedingungen für die Einwilligung
8 Bedingungen für die Einwilligung eines Kindes in Bezug auf Dienste der Informationsgesellschaft
13 Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person
14 Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden
15 Auskunftsrecht der betroffenen Person
16 Recht auf Berichtigung
17 Recht auf Löschung („Recht auf Vergessenwerden“)
18 Recht auf Einschränkung der Verarbeitung
20 Recht auf Datenübertragbarkeit
21 Widerspruchsrecht
24 Verantwortung des für die Verarbeitung Verantwortlichen
25 Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen
28 Auftragsverarbeiter
29 Verarbeitung unter der Aufsicht des Verantwortlichen oder des Auftragsverarbeiters
30 Verzeichnis von Verarbeitungstätigkeiten
32 Sicherheit der Verarbeitung
33 Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde
35 Datenschutz-Folgenabschätzung
36 Vorherige Konsultation
37 Benennung eines Datenschutzbeauftragten
44 Allgemeine Grundsätze der Datenübermittlung

von zentraler Bedeutung.
Es ist grundsätzlich empfehlenswert, die DS-GVO in der Gesamtfassung zunächst einmal zu erkunden und die einzelnen Artikel, die auf das eigene Unternehmen Anwendung finden, gesondert mit Kommentarwerken in den Fokus zu nehmen.

Unter dem folgenden Link erreichen Sie die deutschsprachige Ausgabe der DS-GVO auf der Plattform EUR-Lex (PDF):

http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=DE

Impressum:

Herausgeber:
Datenschutz | Einfach | Digital | Gestalten
eine Initiative der
Marc Weber Management GmbH

Autor:
Marc Weber

Bezugsquelle:
Marc Weber Management GmbH
Lackerbauerstraße 23
81241 München
www.datenschutz-einfach-digital-gestalten.de
datenschutz@marcweber.de
Telefon 089 66 62 86 0
Fax 089 66 62 86 25

Stand:
November 2017

Bildnachweis:
Titelseite: Grundgrafik mohamed1982eg – pixabay, Modifizierung durch Marc Weber Management GmbH