Umsetzung der Datenschutz-Grundverordnung (DSGVO)

Ein Überblick über die Dinge, die **Unternehmen** wirklich umsetzen müssen (und die weh tun können)…

Was ändert sich nicht?

Die Datenschutz-Grundverordnung (DSGVO) ändert vieles, aber vieles bleibt auch gleich…

Ab dem 25. Mai 2018 gilt in der Europäischen Union die DSGVO. Sie ersetzt das bisherige deutsche Datenschutzrecht. Mit wenigen Ausnahmen: Es wird zwar auch am 25. Mai 2018 ein neues Bundesdatenschutzgesetz (BDSG) in Kraft treten. Dies beinhaltet jedoch nur bestimmte Bereiche des Datenschutzrechts, in dem die Mitgliedsstaaten eigene Regelungen zum „Ausfüllen" der DSGVO treffen dürfen.

Ob und unter welchen Voraussetzungen personenbezogene Daten verarbeitet werden dürfen, ändert sich im Vergleich zum bisherigen deutschen Datenschutzrecht nur geringfügig. Wie bisher dürfen Daten mit der DSGVO – vereinfacht dargestellt – in nachfolgenden Konstellationen verarbeitet werden:

1. Die Datenverarbeitung ist erforderlich, um Pflichten aus einem **Vertragsverhältnis** mit dem Betroffenen zu erfüllen. Oder sie ist zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage des Betroffenen erfolgen.
2. Es liegt eine wirksame **Einwilligung** des Betroffenen vor.
3. Es gibt eine **gesetzliche Pflicht** zur Datenverarbeitung (z.B. eine Aufbewahrungspflicht)
4. Die Datenverarbeitung ist erforderlich, um **lebenswichtige Interessen** der betroffenen Person oder einer anderen natürlichen Person zu schützen.
5. Die Datenverarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen der betroffenen Person (oder seine gesetzlich eingeräumten „Datenschutzrechte") überwiegen (Datenverarbeitung auf Basis einer **Interessenabwägung**).

Was ändert sich?

Die Hauptgründe für Unternehmen, sich JETZT um die Umsetzung der DSGVO kümmern (zu müssen), sind:

- ➡ DSGVO-Verstöße können mit **Bußgeldern von bis zu 20 Millionen Euro** (oder bis zu 4% des weltweiten Jahresumsatzes) geahndet werden.
- ➡ Die DSGVO ist **„hartes Compliance-Recht**". Die Nichteinhaltung kann u.U. zur **persönlichen Haftung** von vertretungsberechtigten Personen von Kapitalgesellschaften führen.

Niemand kann derzeit genau abschätzen, wie sich die Situation bei der Verhängung von Bußgeldern im Hinblick auf die Quantität und vor allem auch die Höhe der Bußgelder entwickeln wird.

Neu ist in der DSGVO jedoch die sog. Rechenschaftspflicht („Accountability-Prinzip"), das sich aus Art. 2 DSGVO ergibt. Aus diesem ergibt sich, dass die Einhaltung der Vorgaben der DSGVO vom Unternehmen **nachgewiesen** werden können muss.

Mit Blick auf die erheblichen Bußgeldrisiken sollten Vorstände bzw. Geschäftsführer von Kapitalgesellschaften (§§ 91 Abs. 2, 93 Abs. 1 AktG und § 43 Abs. 1 GmbHG) Risikovorsorge treffen und hierfür geeignete „**Managementsysteme**" einrichten, um das Risiko der persönlichen Haftung auszuschließen oder zumindest zu minimieren.

Aber **auch Personengesellschaften** sind verpflichtet, ein Datensicherheits- und Datenschutzmanagementsystem einzurichten, um die Vorgaben der DSGVO einzuhalten. Sie sollten das schon tun, um das zivilrechtliche Haftungsrisiko zu minimieren. Das Vorhalten eines standardisierten Datensicherheits- und Datenschutzmanagementsystems kann wesentlich dazu beitragen, dass der haftungsrelevante Vorwurf der (einfachen und groben) **Fahrlässigkeit** besser ausgeschlossen werden kann.

Welche Änderungen sind noch relevant?

- ➡ Künftig werden bei risikoreichen Datenverarbeitungen vorgelagerte **Datenschutz-Folgenabschätzungen** durchgeführt werden **müssen**
- ➡ Verschärfte **Meldepflichten** bei Datenpannen
- ➡ Wesentlich verschärfte **Informationspflichten** gegenüber Betroffenen: Datenschutzhinweise in Formularen, Internetseiten etc. müssen überarbeitet werden.

Datenschutzmanagement

Die Lösung?

In Teilbereichen sieht die DSGVO zwingend eine Art von Qualitätsmanagement vor. Prinzipiell ist jedem Unternehmen empfohlen, ein Datenschutzmanagementsystem (DSMS) einzurichten. Aber wie geht das?

Im Bereich der Datensicherheit sind weiterhin technische und organisatorische Maßnahmen zur Sicherheit von personenbezogenen Daten zu treffen, die dem Stand der Technik entsprechen. Wie bisher müssen die Maßnahmen umfangreicher sein, wenn der Schutzbedarf der Daten hoch oder sehr hoch ist. Grundsätzlich dürfen bei der Wahl der Datensicherheitsmaßnahmen auch die Implementierungskosten berücksichtigt werden.

Entscheidend im Bereich der Datensicherheit ist jedoch Art. 32 Abs. 1 lit. d) DSGVO. Danach ist ein […**Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung** …] einzurichten.

Das ist nichts anderes als die Pflicht, ein Datensicherheitsmanagementsystem einzurichten. Hierbei sollte auf bewährte Standards des Qualitätsmanagements zurückgegriffen werden. Für den Bereich der Datensicherheit bietet sich die Einhaltung oder Anlehnung an anerkannte Standards (ISO 27001 oder VdS 3473) an, um sicherzustellen, dass das Sicherheitsmanagement den Anforderungen an den Stand der Technik entspricht.

Im Klartext:

- ➡ Die bislang praktizierte Ausführung von technischen und organisatorischen Maßnahmen i.S.d. der Anlage zu § 9 Satz 1 BDSG **reicht künftig nicht mehr aus**.

- ➡ Datensicherheitsmaßnahmen müssen künftig so beschrieben (und eingehalten) werden, dass die **Integrität** und **Vertraulichkeit** der Daten und auch ihre **Verfügbarkeit** gewährleistet sind.

Da die „Rechenschaftspflicht“ aus Art. 5 Abs. 2 DSGVO zudem den Nachweis der Einhaltung der Vorgaben der DSGVO erfordert, ist auch mit Blick auf alle anderen Prozesse im Unternehmen, bei denen personenbezogene Daten verarbeitet werden, eine prozessorientierte Beschreibung und vor allem auch die Vorgabe von Richtlinien zur Einhaltung im Unternehmen **zwingend erforderlich**, wenn Risiken im Unternehmen minimiert werden sollen.

Und sonst noch?

Die DSGVO bringt noch eine ganze Reihe von Änderungen mit sich. Diese führt auch zu weiteren erforderlichen internen Maßnahmen. Zum Beispiel:

- ➡ Überprüfung der Wirksamkeit von **Einwilligungen**. Diese werden ggf. automatisch ab 25.05.2018 unwirksam.
- ➡ Alle **Auftragsdatenverarbeitungsverträge** müssen überprüft und angepasst werden.
- ➡ Datenverarbeitungen sind in einem **Verzeichnis von Verarbeitungstätigkeiten** zu dokumentieren.
- ➡ Die Grundsätze von Datenschutz **durch Technikgestaltung** („Privacy by Design“) und durch **datenschutzfreundliche Voreinstellungen** („Privacy by Default“) sind bei der Auswahl von Hard- und Software und vor allem bei deren Einsatz einzuhalten. Dies gilt insbesondere auch für die Entwicklung bzw. Bereitstellung von Software.
- ➡ Die DSGVO-Vorgaben sind insbesondere auch bei einer **Verarbeitung von Daten im Auftrag** einzuhalten *und* vom Auftragsverarbeiter nachzuweisen.

Das ist eine ganze Menge Arbeit, bei der Unternehmen sicher Unterstützung benötigen können. Bei der Umsetzung ist ein risikobasierter Ansatz zu empfehlen.

Unternehmen sollten sich also vor allem vorab überlegen, wo die größten Risiken in der Datenverarbeitung in Bezug auf die Einhaltung der DSGVO bestehen. Und dann einen entsprechend priorisierten Maßnahmenplan erstellen.

Die Einhaltung der DSGVO ist kein „einmaliger Aufwand“. ***Es ist ein Prozess der kontinuierlichen Verbesserung*****.**