MEMMINGER LLP

Die EU-Datenschutz-Grundverordnung geht am 25. Mai 2018 in den „Echtbetrieb“ – höchste Zeit, Ihr Unternehmen für eine neue Datenschutz-Ära fit zu machen

November 2017

Die Datenschutz-Grundverordnung des Europäischen Parlaments und des Rates („DS-GVO“)[1] macht nun in Kürze ernst. Ab dem 25. Mai 2018 ist sie in allen EU-Mitgliedsstaaten verbindlich, ohne dass es eines Umsetzungsaktes – wie im Falle einer Richtlinie - in das jeweilige nationale Recht bedarf. In Kraft ist die DS-GVO bereits seit Mai 2016. Sie sieht indessen eine zweijährige Schonfrist vor, in der den Normadressaten Gelegenheit gegeben wird, ihre Prozesse, Systeme und Klauselwerke auf die neue Datenschutz-Zeitrechnung auszurichten. Die Länge der Übergangsfrist mag als Indikator für die Komplexität der Maßnahmen gelten, die der Gesetzgeber auf die Unternehmen zukommen sieht. Nachdem 2/3 der Übergangsfrist schon vorüber sind, nimmt der Handlungsdruck derzeit in vielen Unternehmen dramatisch zu. Verabschieden muss man sich von der Vorstellung, notfalls die Lösung eines anderen Marktteilnehmers, der rechtzeitiger ins Handeln gekommen ist, zu übernehmen. Eine „one fits all“-Lösung gibt es nämlich nicht, sondern Art und Umfang der erforderlichen Maßnahmen hängen von den spezifischen Gegebenheiten eines jeden Unternehmens ab.

I. Zweck dieses Urgent Reminder

Die bevorstehende Scharfschaltung der DS-GVO begründet umfangreichen Handlungsbedarf für viele Unternehmen. Dieser kann sich von technischen Änderungen (*Privacy by Design)* bis hin zur Nachverhandlung von Betriebsvereinbarungen erstrecken.

Dieses Papier soll die Entscheidungsträger dafür sensibilisieren, dass im Prinzip kein Tag mehr verschenkt werden darf, will man nicht sehenden Auges schwerwiegende Complianceverstöße riskieren. Gleichzeitig möchte es vor blindem Aktionismus bewahren; noch besteht für die allermeisten Marktteilnehmer kein Grund zur Panik (die durchaus berechtigt wäre, würden besonders exponierte Unternehmen wie Google, Ebay oder Amazon erst jetzt beginnen, sich Gedanken zu machen). Wir helfen gerne dabei, mit einer klar strukturierten Herangehensweise zeitnah zu gesetzeskonformen Lösungen zu gelangen.

II. Worin besteht der wesentliche Anpassungsbedarf?

1. Es bestehen erheblich verschärfte **Dokumentationspflichten** hinsichtlich der Planung und Durchführung von Datenverarbeitungsprozessen zur Ermöglichung des Nachweises der Datenschutzkonformität gegenüber den Aufsichtsbehörden.

2. **Datenschutzerklärungen** müssen erheblich ausgeweiteten Informationspflichten genügen, was in den seltensten Fällen bereits der Fall sein wird.

3. Die formalen Anforderungen an **Einwilligungserklärungen,** speziell die Dokumentationspflichten bezüglich der Freiwilligkeit der Einwilligung, wurden verschärft; ein etablierter Prozess für den jederzeit möglichen Widerruf der Einwilligung ist nun vorgeschrieben.

4. Im Unternehmen vorhandene **Betriebsvereinbarungen** passen in vielen Fällen nicht mehr zu den Anforderungen der

[1] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)

DS-GVO. Einigkeit über den hieraus resultierenden Änderungsbedarf in Bezug auf teilweise schon lange existierende Betriebsvereinbarungen mit den Arbeitnehmervertretern zu erzielen, kann viel Zeit in Anspruch nehmen.

5. Standard-Klauselwerke für **Auftragsdatenverarbeitung** bedürfen in jedem Fall einer Anpassung an die Neuregelungen zur gesamtschuldnerischen Mithaftung des Auftragsdatenverarbeiters und zu dessen eigenen Dokumentationspflichten, die neben denen der Verantwortlichen Stelle künftig bestehen.

6. Auch die Prozesse für den Umgang mit **Datenpannen** müssen im Zweifel neu aufgesetzt werden, etwa zur Einhaltung der in bestimmten Fällen vorgeschriebenen 72-Stunden-Frist zur Information der Aufsichtsbehörden und der Betroffenen.

7. Datenschutzrisiken können am besten minimiert werden, wenn die Mitarbeiter die essentielle Bedeutung dieses Bereichs und die Gefahren, denen er ausgesetzt ist, verinnerlicht haben. Dies erreicht man am besten durch eine **zielgruppengerechte Sensibilisierung** der Mitarbeiter durch Schulungen und andere „**Awareness-Maßnahmen**".

8. Vielfach wird bisher ein formalisiertes Risk-Assessment zur Ermittlung erforderlicher und geeigneter **technisch-organisatorischer Maßnahmen** zum Schutz personenbezogener Daten, wie es die DS-GVO künftig verlangt, nicht einmal in Ansätzen bestehen.

9. Dies gilt in besonderem Maße für die neu eingeführten Anforderungen an Prüfungsstandards und Dokumentationspflichten zur künftig als Teil des Datenschutz-Risikomanagements vorgeschriebenen **Datenschutzfolgenabschätzung.**

10. In Anbetracht des komplexen Zusammenspiels europäischer und nationaler Rechtssetzungsakte gehört ein aktives „**Monitoring**" der gesetzgeberischen Aktivitäten auf allen Ebenen derzeit etwa mit Blick auf Konkretisierungen zum Beschäftigten-Datenschutz oder zu den Kompetenzen und damit korrelierenden Pflichten des Datenschutzbeauftragten, zum Standardrepertoire der zuständigen Abteilungen, um möglichst frühzeitig mit entsprechenden organisatorisch/ technischen Maßnahmen gegensteuern zu können.

III. Fazit

Das eine ordnungsgemäße Umsetzung des vorstehenden Katalogs kein Kinderspiel wird, dürfte allgemeiner Konsens sein. Kombiniert mit einem drastisch erhöhten Bußgeldrahmen für bestimmte Compliance-Verstöße von bis zu 20 Mio. oder 4% des weltweiten Jahresumsatzes beschert uns das sicher spannende Wochen in nächster Zeit. Stellen Sie sich der Herausforderung!

Memminger LLP
Bleichstraße 64-66
60313 Frankfurt am Main

+49 (0) 69 870 047 800
info@memmingerllp.com
www.memmingerllp.com

Kontakt:
Prof. Dr. Wolfgang G. Büchner
Benjamin Schütze