Die Datenschutz-Grundverordnung – eine erste Bestandsaufnahme

Änderungen, Stand der Umsetzung und Auswirkungen für Unternehmen

Die Europäische Datenschutz-Grundverordnung (DSGVO) ist am 25. Mai 2018 in Kraft getreten. Seit nunmehr fast einem Jahr sind Unternehmen mit deren Umsetzung befasst und haben dafür enorme Ressourcen eingesetzt. Dennoch herrscht nach wie vor eine große Unsicherheit, ob sie die Anforderungen erfüllen und was zu tun ist. Der Beitrag befasst sich mit den relevanten Änderungen durch die DSGVO, dem Stand der Umsetzung und den bisherigen Auswirkungen auf die Praxis. Dazu gehören neben der befürchteten Abmahnwelle – insbesondere durch Wettbewerber – ebenso der Umgang mit Bußgeldern und die Aktivitäten der Aufsichtsbehörden. Zudem wird die Rolle des Datenschutzbeauftragten beleuchtet. (Red.)

„Vier Monate nach Fristablauf hadert die deutsche Wirtschaft weiterhin mit der Umsetzung der EU-Datenschutz-Grundverordnung". Das ist das Ergebnis einer repräsentativen Befragung unter mehr als 500 Unternehmen aus Deutschland, die der Digitalverband Bitkom im September 2018 im Rahmen seiner Privacy Conference vorgestellt hat.[1] Laut der Studie hatte zu diesem Zeitpunkt erst ein Viertel der Unternehmen in Deutschland die DSGVO vollständig umgesetzt. Weitere 40 Prozent hatten die Regeln größtenteils umgesetzt, 30 Prozent teilweise. Gerade erst begonnen mit den Anpassungen hatten 5 Prozent der Unternehmen.

Der Datenschutzbeauftragte

Zwingende erste Schritte für die Umsetzung der DSGVO sind die Änderung der Datenschutzerklärung und die Anpassung der internen Dokumentation (Verfahrensverzeichnis und Folgenabschätzung) sowie im Einzelfall die Bestellung eines Datenschutzbeauftragten.

Die Bestellungspflicht eines Datenschutzbeauftragten hat sich durch die DSGVO beziehungsweise das BDSG[2]-neu erweitert. Durch eine Öffnungsklausel in der DSGVO hat der deutsche Gesetzgeber entschieden, dass Unternehmen, die in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen, zur Bestellung eines betrieblichen Datenschutzbeauftragten verpflichtet sind.

Zusätzlich resultiert nach der DSGVO die Verpflichtung des betrieblichen Datenschutzbeauftragten nicht mehr allein aus der Mitarbeiterzahl. Vielmehr sind vor allem Umfang und Art der vollzogenen Verarbeitungstätigkeiten und damit die hieraus für den Betroffenen potenziell erwachsende Risikolage ausschlaggebend. Unternehmen sind jedenfalls zur Bestellung eines Datenschutzbeauftragten verpflichtet, soweit ihre Kerntätigkeit in der Durchführung umfangreicher, regelmäßiger und systematischer Überwachungen von betroffenen Personen besteht. Eine solche systematische Überwachung von Verhalten der betroffenen Personen wird beispielsweise beim Scoring angenommen. Ob bei Unternehmen der Factoring-Branche die Kerntätigkeit in der systematischen Überwachung von betroffenen Personen besteht, ist einzelfallabhängig.

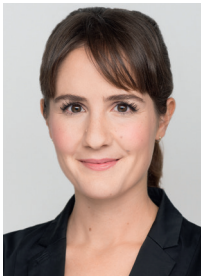
Bei der Bestellung der Datenschutzbeauftragten sollten die Unternehmen

DR. NILS GRUSKE

ist Rechtsanwalt und Counsel bei der Wirtschaftsrechtskanzlei Kallan, Berlin. Zu seinen Beratungsschwerpunkten zählen Datenschutz, gewerblicher Rechtsschutz und IT-Recht.

in

E-Mail:
nils.gruske@kallan-legal.de



CLARA RAPPOLD

ist Rechtsanwältin bei der Wirtschaftskanzlei Kallan, Berlin. Schwerpunkte ihrer Tätigkeit bilden die laufende Beratung von Unternehmen und Startups im allgemeinen Zivil- und Gesellschaftsrecht sowie die Vertragsgestaltung.

in

E-Mail:
clara.rappold@kallan-legal.de

Dieser Artikel ist urheberrechtlich geschützt. Die rechtliche Freigabe ist für den Abonnenten oder Erwerber ausschließlich zur eigenen Verwendung.
Verlag für Absatzwirtschaft GmbH

jedoch stets abwägen, ob sie einen internen oder externen Datenschutzbeauftragten bestellen möchten. Vorteil eines internen Datenschutzbeauftragten ist, dass dieser bereits mit den Prozessen im Unternehmen vertraut ist. Zudem kann sich ein interner Sachverständiger vollständig auf das Unternehmen konzentrieren. Schließlich besteht zu einem im Unternehmen angestellten Datenschutzbeauftragten im Regelfall ein engeres Vertrauensverhältnis als zu Externen.

Die Vorteile bei einem externen Datenschutzbeauftragten liegen zum einen darin, dass dieser sich nicht auf Abberufungs- oder Kündigungsschutz berufen kann – allerdings sind die vereinbarten Vertragslaufzeiten zu beachten. Zudem besteht für das Unternehmen kein Haftungsrisiko aufgrund innerbetrieblichen Schadensausgleichs. In der Regel sind externe Datenschutzbeauftrage erfahrener und arbeiten professioneller, im Gegensatz zum internen Datenschutzbeauftragten ist außerdem keine Einarbeitung nötig.

Vorzüge des Externen

Im Einzelfall können deshalb auch die Kosten bei einem externen Datenschutzbeauftragten niedriger ausfallen. Diese sind unter anderem abhängig von Standort, Reisekosten und der Beschäftigtenzahl im Unternehmen. Zudem ist auf Regelungen im Dienstvertrag zu zusätzlichen Kosten zum Beispiel wegen Audit oder zu zusätzlichen Leistungen zu achten. Ein weiterer Vorteil des externen Datenschutzbeauftragten könnte auch die neutrale Position gegenüber Mitarbeitern im Unternehmen als auch nach außen sein.

Der Trend entwickelt sich zum externen Datenschutzbeauftragten. Das ist wohl vor allem auf die Haftungssicherheit und den besonderen Kündigungsschutz des internen Datenschutzbeauftragten zurückzuführen. Hat ein Unternehmen bereits einen internen Datenschutzbeauftragten bestellt, ist der Entscheidungsspielraum allerdings eingeschränkt, da der bestellte Mitarbeiter besonderen Abberufungsschutz genießt.

Die Abmahnwelle

Vor und seit Inkrafttreten der DSGVO wurde vielfach über eine Abmahnwelle aufgrund von Datenschutzverstößen spekuliert. Eine solche blieb jedoch bislang weitestgehend aus. Es gab einzelne Versuche unmittelbar nach Inkrafttreten der DSGVO, insbesondere wurden einzelne Abmahnungen wegen fehlender beziehungsweise fehlerhafter Datenschutzerklärungen auf den Internetseiten versandt.

Ob Datenschutzverstöße von Wettbewerbern abgemahnt werden können, ist derzeit umstritten. Das Landgericht (LG) Würzburg hat wohl als erstes deutsches Gericht eine Abmahnbarkeit von DSGVO-Verstößen auf Internetseiten festgestellt.[3] Das LG Bochum entschied hingegen, dass Verstöße gegen Artikel 13 DSGVO nicht von Mitbewerbern abgemahnt werden können.[4] Das LG Wiesbaden hat sich der Auffassung des LG Bochum angeschlossen.[5] Am 25. Oktober 2018 entschied das Hanseatische Oberlandesgericht (OLG), Hamburg, sich als erstes Oberlandesgericht für die Abmahnbarkeit von DSGVO-Verstößen.[6] Deshalb ist aber nicht jeder DSGVO-Verstoß automatisch abmahnbar. Voraussetzung ist, dass die betroffene Datenschutzvorschrift „marktverhaltensregelnden Charakter" hat. Diese Frage muss für jede DSGVO-Regelung konkret geprüft werden.

Wegen der unsicheren Rechtslage sollte daher jede Abmahnung und Unterlassungsklage sorgfältig geprüft werden. Insbesondere ist zu prüfen, ob der angebliche Verstoß tatsächlich besteht und ob die angeblich verletzte Norm überhaupt „marktverhaltensregelnden Charakter" hat.

Dem Gesetzgeber ist die Problematik des Abmahnwesens bekannt. So hat der Freistaat Bayern am 26. Juni 2018 im Bundesrat einen Gesetzesantrag eingebracht, mit dem Abmahnungen gegen Datenschutzverstöße eingedämmt werden sollen.[7] Die Intention des Gesetzesentwurfes ist, missbräuchliche Abmahnungen durch (vermeintliche) Wettbewerber im Bereich Datenschutzrecht vorzubeugen und Rechtsunsicherheit zu beseitigen. So sollen laut Gesetzentwurf bei DSGVO-Verstößen Abmahnungen nur durch bestimmte Verbraucherschutzverbände, und nicht mehr durch Wettbewerber, zulässig sein. Darüber hinaus sollen Abmahnungen von bloßen formellen Fehlern, wie fehlerhafter Unterrichtungs- und Mitteilungspflichten gar nicht abmahnfähig sein. Ob und in welcher Form dieser Gesetzesentwurf verabschiedet wird, bleibt abzuwarten.

Praxis der Aufsichtsbehörden

Das Inkrafttreten der DSGVO war auch für die Aufsichtsbehörden eine enorme Belastung. Es war also keine Überraschung, dass die Aufsichtsbehörden anfangs erst einmal mit sich beschäftigt waren. Bislang waren die Behörden überwiegend informatorisch tätig. Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) hat Kurzpapiere zu diversen Themen erstellt. Einige Landesdatenschutzbeauftragte stellen auf ihren Internetseiten verschiedene Kurzinformationen oder Orientierungs- und Praxishilfen zur Verfügung, darunter auch Listen von Verfahren, bei denen eine Folgenabschätzung nötig ist (beispielsweise Mobilitätsdienste/Car Sharing, Bewertungsportale, Inkassodienstleistungen, Soziale Netzwerke).

Die Landesbeauftragte für den Datenschutz Niedersachsen prüft derzeit in einer branchenübergreifenden Querschnittsprüfung, wie gut sich die niedersächsischen Unternehmen bisher auf die DSGVO eingestellt haben. Der Abschlussbericht soll im Mai 2019 vorliegen.

Das erste höhere Bußgeld in Europa wurde von der Datenschutzbehörde in Portugal verhängt. Das Bußgeld von 400 000 Euro soll ein Krankenhaus wegen unzureichenden Zugriffsbeschränkungen bei sensiblen Patienten-

Dieser Artikel ist urheberrechtlich geschützt. Die rechtliche Freigabe ist für den Abonnenten oder Erwerber ausschließlich zur eigenen Verwendung.
Verlag für Absatzwirtschaft GmbH

daten zahlen.[8] In Österreich wurden bisher überwiegend illegale Videoüberwachungen geahndet. Die dort bislang höchste Geldbuße traf ein Wettlokal, das wegen illegaler Videoüberwachung mit 4800 Euro zur Kasse gebeten wurde.[9]

Erste Bußgelder

Am 21. November 2018 verhängte nun auch der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg das erste in Deutschland bekannt gewordene Bußgeld. Das soziale Netzwerk „Knuddels" muss 20000 Euro zahlen, da es die personenbezogenen Daten seiner Kunden nicht ausreichend gesichert hat. Die Plattform war Opfer eines Hackerangriffs geworden. In dem Fall hat das betroffene Unternehmen davon profitiert, dass es seinen Meldepflichten unverzüglich und in umfassender Weise nachkam.[10] Der Verstoß gegen die DSGVO hätte ansonsten deutlich größere Konsequenzen nach sich ziehen können.

Nach einer Umfrage des Handelsblatts unter mehreren Landesdatenschutzbeauftragten seien inzwischen zahlreiche Bußgeldverfahren eingeleitet worden.[11] In Nordrhein-Westfalen ging es dabei insbesondere um Fälle, in denen die Behörde von den angeschriebenen Verantwortlichen keine Auskünfte erhalten habe sowie um den „unrechtmäßigen Einsatz" von Mini-Kameras, sogenannten Dashcams. Laut der Pressesprecherin der Berliner Datenschutzbehörde beschwerten sich Betroffene besonders stark über Unternehmen, die Selbstauskünfte nicht oder nicht richtig erteilten oder den Löschansprüchen von Betroffenen nicht nachkämen sowie über unerwünschte E-Mail-Werbung.

Zudem beträfen die Beschwerden vielfach den Einsatz von Cookies oder die Datenschutzerklärungen von Internetauftritten. „Wir erhalten sehr viele Hinweise zu Webseiten, die gar keine oder offensichtlich mangelhafte Datenschutzhinweise enthalten", erklärte die Behördensprecherin dem Handelsblatt.[12]

Verfolgung von Verstößen

Die vollständige Umsetzung der DSGVO ist zwingend erforderlich. Die oben genannten ersten Schritte – Datenschutzerklärung aktualisieren, Verfahrensverzeichnis und Folgeabschätzung erstellen, Datenschutzbeauftragten benennen – sollten umgesetzt sein. Eine offizielle Regelung zu einer „Karenzzeit" gibt es nicht, hierauf sollten sich Unternehmen also nicht verlassen. Die Behörden scheinen nach der Einarbeitungsphase nun größere Kapazitäten für die Verfolgung von DSGVO-Verstößen zu haben. Die Aufsichtsbehörden sind zudem europarechtlich zur Durchsetzung der DSGVO verpflichtet, sonst droht Deutschland ein Vertragsverletzungsverfahren.

Unternehmen ist also zu raten, sich umfassend in Hinblick auf die Vorschriften der DSGVO abzusichern, um Datenschutzverstöße im Voraus zu vermeiden. Kommt es dennoch zu einem Verstoß, sollte schnellstmöglich reagiert werden, um Konsequenzen abzufedern und Haftungsrisiken zu minimieren.

Fußnoten

1) Vgl. Susanne Dehmel, Barbara Thiel, Präsentation: „Vier Monate DSGVO – wie weit ist die deutsche Wirtschaft?" (27. September 2018), www.bitkom.org
2) BDSG = Bundesdatenschutzgesetz.
3) LG Würzburg, Beschluss vom 13. September 2018, Az. 11 O 1741/18.
4) LG Bochum, Urteil vom 7. August 2018, Az. I-12 O 85/18.
5) LG Wiesbaden, Urteil vom 5. November 2018, Az. 5 O 214/18.
6) OLG Hamburg, Urteil vom 25. Oktober 2018, Az. 3 U 66/17.
7) BR-Drs. 304/18.
8) Martin Holland, „DSGVO-Verstoß: Krankenhaus in Portugal soll 400000 Euro zahlen" (23. Oktober 2018), in: www.heise.de
9) Muzayen Al-Youssef, „Bislang vier Strafen wegen DSGVO-Verstößen seit Mai" (23. November 2018) in: https://derstandard.at
10) tik/LTO-Redaktion, „Datenschutzverfahren gegen Knuddels abgeschlossen" (22. November 2018), in: www.lto.de/recht/nachrichten
11) Dietmar Neuerer, „Unternehmen drohen Bußgelder in „erheblichem Umfang" (30. Oktober 2018), in: www.handelsblatt.com/politik
12) Dietmar Neuerer, „Unternehmen drohen Bußgelder in „erheblichem Umfang" (30. Oktober 2018), in: www.handelsblatt.com/politik

risklytics

Die digitale
MaRisk Lösung

Die Software risklytics deckt alle quantitativen Aspekte Ihres MaRisk-Risikomanagements in Leasing- und Factoringfirmen ab:

- Risikotragfähigkeitsrechnung
- Limitsystem
- Frühwarnsystem
- Automatische Berichterstellung
- Plausibilitätsprüfungen
- Internes Kontrollsystem
- Daten-Schnittstelle
- Stresstests

risklytics GmbH
Universität des Saarlandes
Campus Starterzentrum 1
66123 Saarbrücken
Tel: 0681 302 64977
www.risklytics.de

Dieser Artikel ist urheberrechtlich geschützt. Die rechtliche Freigabe ist für den Abonnenten oder Erwerber ausschließlich zur eigenen Verwendung.
Verlag für Absatzwirtschaft GmbH