24878

ZVertriebsR
Zeitschrift für Vertriebsrecht

www.ZVertriebsR.de

Handelsvertreterrecht
Vertragshändlerrecht
Vertriebskartellrecht
Franchiserecht
Online-Vertriebsrecht

C.H.BECK

2/2017

S. 69–136, 21. März 2017
6. Jahrgang

Aus dem Inhalt

P050201702

Rechtsanwalt Dr. Hermann Lindhorst*

Wachgeküsst – Datenschutz im Franchising nach der EU-Datenschutzgrundverordnung

Bisher führte der Datenschutz im Allgemeinen und im Franchising im Besonderen ein Mauerblümchendasein: Jeder wusste, dass er zu beachten ist, tat aber nur so viel, wie gerade notwendig. Im Wissen um das in der täglichen juristischen Praxis vorhandene Vollzugsdefizit, wonach Datenschutzverstöße nur selten und nicht besonders intensiv geahndet werden, war die Bereitschaft mit der Auseinandersetzung datenschutzrechtlicher Themen gering, was durch die komplizierte, sprachlich-redaktionell mangelhafte Fassung des Bundesdatenschutzgesetzes (BDSG) befördert wurde. Was ändert sich nun durch die neue EU-Datenschutzgrundverordnung (DS-GVO), deren Vorschriften gegenüber jedem Unternehmen unmittelbar gelten und die am 25.5.2018 anzuwenden sind?

I. Einführung: Datenschutz und Franchising bis zur DS-GVO

Die bisherige datenschutzrechtliche Praxis für Franchisezentralen beschränkte sich neben allgemeinen datenschutzrechtlichen Fragen, die jedes Unternehmen einzuhalten hat, wie z.B. einer wirksamen Datenschutzerklärung für die Website oder Richtlinien zur privaten Nutzung von E-Mail und Internet (vor allem mit Blick auf den Beschäftigtendatenschutz) bisher vor allem auf Marketingfragen, wie z.B. den Möglichkeiten der rechtmäßigen Einwilligung in die Zusendung von Werbung in Verbindung mit Kundenkarten.[1] Insbesondere im Einzelhandel und der Gastronomie tätige Franchiseunternehmen müssen sich darüber hinaus verstärkt mit § 6b BDSG auseinandersetzen, der die Zulässigkeit der Videoüberwachung öffentlicher Räume regelt.[2] Verbreitet sind auch die für beide Seiten grundsätzlich vorteilhaften Auftragsdatenverarbeitungsverträge, die, wenn sie § 11 BDSG entsprechend vereinbart werden, eine datenschutzrechtlich relevante Übermittlung legitimieren können. Zwischen Franchisegeber und Franchisepartner scheidet allerdings regelmäßig die Möglichkeit eines solche Auftragsdaten-

* Der Verfasser ist Rechtsanwalt und Fachanwalt für IT-, Urheber- und Medienrecht bei SCHLARMANNvonGEYSO, Hamburg sowie assoziierter Experte des Deutschen Franchise-Verbands e.V..

1 Vgl. § 7 UWG sowie zuletzt OLG Frankfurt am Main, 28.07.2016 – 6 U 93/15.

2 Hierbei steht die Überwachung der eigenen Mitarbeiter im Vordergrund, hierzu zuletzt BAG, U. v. 22.9.2016, Az. 2 AZR 848/15, aber auch Aufzeichnungen zur Aufklärung von z.B. Einbrüchen.

verarbeitungsvertrags aus, da der Auftragsdatenverarbeiter gem. § 11 vertraglich besonders eng an den Weisungen des Auftraggebers gebunden sein muss (mit Weisungsrechten) und ihm jeder Ermessens- und Entscheidungsspielraum fehlt.[3]

Demgegenüber sind datenschutzrechtliche Regelungen in Franchiseverträgen kaum anzutreffen. Die franchiserechtliche Literatur weist kaum spezielle Aufsätze zu Datenschutzthemen aus,[4] was möglicherweise auch am schwer zugänglichen Datenschutzrecht mit einem an vielen Stellen sprachlich unklaren BDSG liegen mag. Jüngstes Beispiel dafür ist ein Urteil des Bundesarbeitsgerichts, in dem der Wortlaut von § 32 BDSG, der den praktisch enorm wichtigen Beschäftigtendatenschutz regelt, als „*verunglückt*" bezeichnet hat.[5] Für eine gewisse Aufmerksamkeit sorgt nach wie vor – aufgrund zahlreicher Abmahnungen – die Frage, ob die Verletzung datenschutzrechtlicher Normen auch wettbewerbsrechtlich abgemahnt werden kann,[6] was aber nicht darüber hinwegtäuschen darf, dass datenschutzrechtliche Themenfelder im Franchiserecht oder Klauseln in Franchiseverträgen eher eine untergeordnete Rolle spielen. Neben den o.a. Marketingfragen[7] betreffen sie vor allem die Übermittlung und Auswertung von Kassendaten oder die Beziehungen zwischen Franchisegeber und -nehmer einerseits sowie den jeweiligen Systemlieferanten und -dienstleistern (sowie andere Logistikpartner) andererseits.[8]

Eine Ausnahme dieser datenschutzrechtlichen Zurückhaltung stellen sicherlich börsennotierte Großkonzerne dar, von denen es auch einige gibt, die als Franchisesystem organisiert sind. Diese Unternehmen sind im Rahmen der seit Jahren bereits geführten Diskussion um „Compliance" in der Pflicht, den Datenschutz ernst zu nehmen und dafür zu sorgen, dass die entsprechenden Vorschriften auch umgesetzt werden. Doch auch im Rahmen der Compliance-Diskussion hält der Datenschutz im Franchising bisher eher einen Dornröschenschlaf und wird in den entsprechenden Aufsätzen nicht näher thematisiert.[9]

II. Die EU-Datenschutzgrundverordnung[10]

1. Entstehung

Nach Vorstellung der EU-Datenschutzreform durch die Kommission Anfang 2012 wurde die DS-GVO nach überaus intensiven Beratungen durch das Europäische Parlament verabschiedet. Nach weiteren zwei Jahren, die ebenso intensiv von Lobby-Verbänden und Regierungen der EU-Mitgliedstaaten begleitete wurden,[11] beschloss der EU-Rat die verbindliche Fassung der Richtlinie, die im April 2016 im EU-Amtsblatt veröffentlicht wurde. Am 25.05.2018 werden die Vorschriften geltendes Recht sein und sind als Verordnung (im Gegensatz zu einer EU-Richtlinie, die sich an die Mitgliedstaaten richtet und von diesen erst noch umgesetzt werden müsste) unmittelbar gegenüber jedem Unternehmen rechtswirksam.

Die schiere Masse an Text sowie die mit der EU-Datenschutzgrundverordnung neu eingeführten Regelungen sind für sich allein genommen bereits beeindruckend; insgesamt spiegeln 171 Erwägungsgründe und 99 Artikel einen der intensivsten Gesetzgebungsprozesse der Europäischen Union überhaupt wider,[12] zumal viele aufgrund der höchst unterschiedlichen Interessenlagen – nicht nur zwischen Industrie und Datenschutzbefürwortern, sondern auch zwischen den Mitgliedstaaten – befürchtet hatten, es werde zu keiner Einigung kommen.[13]

2. Wesentliche Inhalte

Von den vielen neuen Regelungen werden hier nur einige wenige herausgegriffen, die sich insbesondere an Unternehmen richten.[14]

a) Deutlich umfassendere Sanktionsmöglichkeiten

Sehr einschneidende Änderungen betreffen zunächst die Regelungen zu Sanktionen, denn zum einen wurde der Bußgeldrahmen deutlich erhöht: Nunmehr sind für Unternehmen Bußgelder von bis zu 4% des globalen Umsatzes möglich.[15] An Verstößen beteiligte natürliche Personen müssen mit Geldbußen rechnen, die bis zu € 20 Mill. betragen können. Da bei Unternehmen die Umsätze des Gesamtkonzerns maßgeblich sein werden, sind durchaus dreistellige Millionenbeträge als Geldbuße möglich, ähnlich wie das bisher nur bei kartellrechtlichen Verstößen der Fall war. Künftig sind dann übrigens neben materiellen auch immaterielle Schäden zu erstatten, die auf Verstößen gegen die Verordnung beruhen. [16]

---

3 So für den Handelsvertreter *Kugler* ZVertriebsR 2015, 222; dies gilt ebenso für ein franchiserechtlich ausgestaltetes Vertriebsverhältnis (so *Büser*, a.a.O., S. 218), u.a. weil der Franchisepartner rechtlich selbständiges und vom Franchisegeber verschiedenes Unternehmen ist. In den meisten Fällen sind Übermittlungen aus Sicht des Endkunden gem. § 28 Abs. 1 S. 1 Nr. 2 BDSG legitimiert (*Büser*, a.a.O., S. 218); für die in der Praxis wichtigen marketingrechtlichen Konstellation – etwa dem Versand von Werbemails – gilt das allerdings nicht.

4 Vgl. den ersten Aufsatz hierzu vor über zwanzig Jahren *Büser*, Rechtliche Probleme im Rahmen der Datenübermittlung beim Franchising, BB 1997, 213. Die einzigen systematischen Darstellungen der datenschutzrechtlichen Bezüge zum Franchiserecht finden sich bei *Mietzel* in *Giesler/Nauschütt*, Franchiserecht, 3. Aufl. 2016, Kap. 14 sowie *Thoma* in *Metzlaff* (Hrsg.), Praxishandbuch Franchising, 2003, § 19. Zu datenschutzrechtlichen Fragen beim Einsatz von Handelsvertretern vgl. *Kugler*, Datenschutzrechtliche Fragen beim Einsatz von Handelsvertretern, ZVertriebsR 2015, 219.

5 Vgl. BAG, U. v. 22.9.2016, Az. 2 AZR 848/15 Rz. 30. Ebenso *Büser*, a.a.O. S. 216, mit Kritik an der Fassung von § 28 BDSG.

6 Klassisch etwa die Auseinandersetzung zwischen OLG Hamburg, Urt. v. 27.6.2013 – 3 U 26/12 (für UWG-Verstoß) und KG, U. v. 29.4.2011 – 5 W 88/11 (gegen UWG-Verstoß) zu § 13 TMG.

7 Sowohl off-, vor allem aber auch online; vgl. *Krüger/Peintinger* in *Martinek/Semler/Flohr* (Hrsg.), Handbuch des Vertriebsrechts, 4. Aufl. 2016, § 36 Rn 299-352. Vor allem im Einzelhandel gewinnen technische Verfahren zur Marketingunterstützung rasant an Bedeutung; hierzu zählt nicht nur das Zurverfügungstellen von freien WLAN-Verbindungen, sondern auch die „Near Field Communication" (NFC) insb. bei Zahlungsvorgängen oder Loyalty-Apps mit sog. „Beacons" (die auf einen auf Bluetooth Low Energy (BLE) basierenden Sender reagieren).

8 Vgl. hierzu *Mietzel* a.a.O., Rz. 11 ff. sowie *Thoma* a.a.O., Rz. 35 ff.

9 Vgl. zuletzt *Waldzus*, Compliance im Franchising: Darf's ein bisschen mehr sein? – Neue Herausforderungen für Franchisesysteme im Licht aktueller Rechtsprechung, BB 2016, 515 ff. oder *Metzlaff/Stauber*, Compliance in Franchisesystemen, in: Jahrbuch Franchising 2011, S. 17 ff.

10 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rats 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), abrufbar unter http://eur-lex.europa.eu/legal-content/ET/TXT/PDF/?uri=CELEX:32016R0679&from=DE .

11 Die Stellungnahme des Deutschen Franchise-Verbands e.V. ist über http://tinyurl.com/DFV-DSGVO-E abrufbar.

12 Sehr anschaulich verdeutlicht die Dokumentation „Im Rausch der Daten" den Entstehungsprozess der DS-GVO über insgesamt mehr als sechs Jahre, vgl. http://www.democracy-film.de/ . Der Film ist uneingeschränkt sehenswert, insbesondere für diejenigen, die den Datenschutz *bisher* als übertriebene, bürokratisch-administrative Last empfunden haben, was bisher so auch auf den Autor zutraf.

13 Einer der ausschlaggebenden Umstände für die letztlich erfolgreiche Verabschiedung der DS-GVO waren die Vorgänge um den US-amerikanischen Whistleblower *Edward Snowden*, der im Sommer 2013 die NSA-Affäre auslöste und so eine gesteigerte Datenschutzsensibilisierung auslöste.

14 Im Übrigen sei auf den Überblick verwiesen bei *Schantz*, Die Datenschutz-Grundverordnung – Beginn einer neuen Zeitrechnung im Datenschutzrecht, NJW 2016, 1841.

15 Art. 83 DS-GVO.

16 Vgl. Art. 82 DS-GVO. Zusätzlich können nach dieser Regelung auch Auftragsdatenverarbeiter in Haftung genommen werden.

Anders als bisher werden auch Verstöße gegen Vorschriften zum Schutz der Datensicherheit sanktioniert.[17]

Zum anderen sollen nun auch Verbände – mehr noch als bisher – datenschutzrechtliche Verstöße verfolgen dürfen, so dass sich z.B. Verbraucherverbände dem Thema Datenschutz verstärkt annehmen werden. Schließlich sind die Dokumentations- und Nachweispflichten mit der DS-GVO deutlich erhöht worden – wer dagegen verstößt und – etwa im Rahmen der Auftragsdatenverarbeitung – bestimmte Nachweise nicht erbringen kann, haftet für diese Datenschutzverstöße.

Allerdings kann sich datenschutzkonformes Handel künftig auch auszahlen: Während es Unternehmen früher kaum zu vermitteln war, dass sie von der Einhaltung datenschutzrechtlicher Vorschriften auch greifbare Vorteile haben, gilt das nach den neuen Vorschriften nunmehr auch ausdrücklich: So ist bei der Bemessung einer datenschutzrechtlichen Sanktion zu berücksichtigen, inwiefern das jeweilige Unternehmen datenschutzrechtliche Sicherungsvorkehrungen getroffen hat. Das bedeutet konkret, dass ein Unternehmen, dass z.B. nicht nur einen Datenschutzbeauftragten hat, sondern auch ein im Wesentlichen korrektes datenschutzrechtliches Grundniveau einhält, deutlich bessere Argumente in einer datenschutzrechtlichen Konfliktsituation haben wird als ein Unternehmen, dass in diesen Bereichen grundsätzlich schlecht aufgestellt ist oder den Datenschutz gar gänzlich ignoriert. Ähnliche Vorteile sieht die DS-GVO vor, wenn das Unternehmen seine Technik besonders datenschutzfreundlich ausgestaltet („privacy by design“) oder datenschutzkonforme Voreinstellungen gewählt hat („privacy by default“).[18]

b) Stärkere Stellung des Datenschutzbeauftragten

Mehr noch als bisher wird der Datenschutzbeauftragte im Unternehmen die zentrale Ansprechperson für alle Belange des Datenschutzes. Zu seinen Aufgaben gehört die Unterrichtung und Beratung des Unternehmens, des Auftragsverarbeiters und der Beschäftigten beim Datenschutz, die Überwachung der DS-GVO sowie die Überwachung der Zuweisung von Zuständigkeiten, Schulungen und Überprüfungen (hier sind auch Zertifizierungen zu nennen, deren Bedeutung ebenfalls erheblich ansteigen wird).[19] Zudem bewertet er Fragen zur Datenschutz-Folgenabschätzung (s. sogleich) und ist Ansprechpartner der jeweiligen Aufsichtsbehörde. Mit der neuen DS-GVO gehen erhöhte Dokumentationspflichten einher, die der Datenschutzbeauftragte erfüllen muss.

Da der Datenschutzbeauftragte bisher nur auf die Einhaltung datenschutzrechtlicher Regelungen „hinwirken“ musste, was nun nicht mehr der Fall ist, rechnen viele damit, dass sich die Haftungsrisiken für Datenschutzbeauftragte mit der DS-GVO erhöhen.[20]

c) Datenschutz-Folgenabschätzung

Dieser Bereich ist – insbesondere für große Unternehmen – eine der wesentlichsten Neuerungen[21] und sorgt dafür, dass diese Unternehmen bereits ihre Budgets erhöht haben, um nur für diese Folgenabschätzung neue Mitarbeiter einzustellen:

Hat ein datenschutzrechtlich relevanter Vorgang *voraussichtlich hohe Risiken* für die persönlichen Rechte und Freiheiten der davon betroffenen Personen zur Folge, so muss das entsprechende Unternehmen eine umfassende und aufwendige Datenschutz-Folgenabschätzung durchführen.[22] Hierbei sollen insbesondere Eintrittswahrscheinlichkeit und Schwere möglicher Risiken bewertet werden. Das Unternehmen soll auch Art, Umfang, Umstände, verfolgte Zwecke sowie Ursachen möglicher Risiken bewerten. Dabei soll es auch Maßnahmen, Garantien und Verfahren prüfen, mit denen Unternehmen bestehende Risiken eindämmen und die sonstigen Vorgaben der Verordnung einhalten können; hierzu gehört auch die Hinzuziehung der datenschutzrechtlichen Aufsichtsbehörde.

Notwendig ist also nicht nur zunächst die Einschätzung, ob ein Unternehmen eine solche Folgenabschätzung vornehmen muss, sondern auch deren Umsetzung. Möglicherweise werden die Datenschutzbehörden hierzu noch Stellungnahmen veröffentlichen mit Positiv- und Negativlisten, an denen sich die Unternehmen dann orientieren können.[23] Da bisher kein Standard für die genauen Inhalte einer Datenschutz-Folgenabschätzung besteht, wird getreu dem Motto „viel hilft viel“ dazu geraten, die Folgenabschätzung im Zweifel eher umfangreicher ausfallen zu lassen.[24]

d) Erweiterte Informationspflichten

Unternehmen müssen betroffene Personen vor der Verarbeitung ihrer personenbezogenen Daten „*in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer einfachen und klaren Sprache*“ unterrichten.[25] Art. 12 bis Art. 15 DS-GVO führen dazu umfangreiche Unterrichtungsrechte betroffener Personen und Auskunftspflichten an, die umfangreicher sind als die bislang geltenden Vorschriften des BDSG.

e) Weitreichendere Löschpflichten

Die erweiterten Löschpflichten können insbesondere zwischen Franchisezentrale, Franchisepartner und Kunden von Relevanz sein:

Wenn ein Unternehmen zu löschende Daten öffentlich gemacht hat, muss es andere Verantwortliche, die diese Daten verarbeiten, davon informieren, dass eine betroffene Person von ihnen die Löschung „*aller Links zu oder aller Kopien oder Replikationen von diesen personenbezogenen Daten*“ verlangt hat.[26] Zwar gibt es Ausnahmen von diesen Löschpflichten, die aber deutlich enger gefasst sind als im bisherigen Recht nach dem BDSG.

f) Datenschutz im Konzern: Nach wie vor kein Konzernprivileg, aber Erleichterungen

Die DS-GVO enthält – ebenso wie das BDSG – kein Privileg zugunsten von Konzernen. Sie differenziert aber nicht zwischen Datenverarbeitungen für eigene Zwecke und Datenverarbeitungen zur Wahrung berechtigter Interesse Dritter und erlaubt damit solch eine Datenverarbeitung, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person überwiegen. Es

17 Vgl. Art. 32 DS-GVO.
18 Art. 25 DS-GVO.
19 Vgl. Art. 39 DS-GVO.
20 Vgl. *Wybitul*, BB 2017, S. 185.
21 Vorher gab es bereits eine sog. „Vorab-Kontrolle“ nach dem BDSG, die aber ihren Voraussetzungen nach weniger einschneidend war als die nun eingeführte Folgenabschätzung.
22 Vgl. Art. 35 DS-GVO.
23 Art. 35 Abs. 4 bis Abs. 6 DS-GVO.
24 Vgl. *Wybitul*, Checklisten zur DS-GVO, BB 2016, 2307 mit dem Hinweis, dass die Folgenabschätzung auch als wichtiger Bestandteil des Risikomanagements in Bezug auf den Datenschutz genutzt werden kann.
25 Art. 12 DS-GVO.
26 Art. 17 DS-GVO.

bleibt abzuwarten, ob aus einem Erwägungsgrund, der einen Konzern weniger eng definiert als bisher, evtl. weitere Vorteile zugunsten von Franchiseunternehmen gezogen werden können.[27]

g) Unzureichende bzw. fehlende Regelungen

Trotz der o.a. Neuerungen bleiben viele aktuell diskutierte datenschutzrechtliche Fragen noch unzureichend geregelt. Dies gilt u.a. etwa für den wichtigen und praktisch hoch relevanten Beschäftigtendatenschutz.

Leider fehlen auch Regelungen bzw. klare Aussagen zu diversen z.T. intensiv diskutierten datenschutzrechtlichen Problemstellungen, wie z.B. sog. Big-Data-Anwendungen oder Scoring/Profiling. Einige davon werden zwar definiert, aber nicht näher geregelt oder nur an vereinzelten Stellen genannt. Schließlich enthält die DS-GVO zwar zahlreiche Bestimmungen zur Übermittlung von Daten in Drittländer.[28] Nach wie vor fehlt es aber z.B. an einer rechtssicheren Grundlage für die Übermittlung von Daten in die USA.[29]

3. Deutsches Anpassungs- und Umsetzungsgesetz

Da die DS-GVO als Verordnung unmittelbar gilt und eigentlich keiner Umsetzung bedürfte, wäre ein Umsetzungsgesetz eigentlich nicht erforderlich. Allerdings enthält die DS-GVO in sehr vielen Bereichen Regelungen, die von den einzelnen Mitgliedstaaten, und auch den dortigen Datenschutzbehörden, konkretisiert oder ergänzend geregelt werden können; zu berücksichtigen ist in diesem Zusammenhang auch, dass die DS-GVO ohnehin an vielen Stellen auslegungsbedürftige oder unbestimmte Rechtsbegriffe enthält. Dieses stellt einen Hauptkritikpunkt an der DS-GVO dar, denn eigentlich wäre eine bestmögliche Harmonisierung sicherlich dann erreicht, wenn es keinerlei nationaler Umsetzung mehr bedürfte.

Das Bundeskabinett hat am 1.2.2017 den „Entwurf eines Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU)“ verabschiedet. Bereits wenige Tage nach Veröffentlichung hat es hierauf z.T. harsche Kritik gegeben, die sich nicht nur auf den übermäßigen Umfang bezieht, sondern auch auf die offenbar beabsichtigte Änderung von Regelungsbereichen, die von der DS-GVO eigentlich bereits vorgegeben waren.[30] Es ist nicht gesichert, ob die (zeitlichen) Anstrengungen des Gesetzgebers ausreichen werden, damit das Gesetz noch in dieser Legislaturperiode verabschiedet werden kann.[31] Ist das nicht der Fall, verfällt der bisherige Gesetzesentwurf des sog. Diskontinuität, was mit Rechtsunsicherheit verbunden wäre.[32]

Inhaltlich schlägt der Gesetzgeber ein neu gestaltetes BDSG vor. Bei einigen Regelungen belässt es der Entwurf beim Status Quo, was etwa für die Mitarbeiteranzahl gilt, aufgrund derer die Bestellung eines Datenschutzbeauftragten notwendig ist (zehn und mehr).

III. Drei Handlungsempfehlungen für Franchisesysteme

1. Herstellung eines datenschutzrechtlichen Mindestniveaus

Unabhängig von den ab dem 25.5.2018 geltenden neuen Regelungen sollten alle Unternehmen als erstes prüfen, ob sie zumindest einen gewissen datenschutzrechtlichen Mindeststandard einhalten.

Hierzu gehören insbesondere ein Datenschutzbeauftragter, der sämtliche datenschutzrelevanten Bereiche des Unternehmens kritisch prüft und dafür sorgt, dass z.B. in Arbeitsverträgen oder unternehmensinternen Richtlinien datenschutzrechtliche Sachverhalte korrekt geregelt werden.

Außerdem gehört die Herstellung einer datenschutzrechtlichen Sensibilisierung aller Mitarbeiter zu diesem Mindeststandard, bei dem – etwa durch regelmäßige Schulungen – die Grundlagen des Datenschutzrechts vermittelt werden. Ganz allgemein gilt nach wie vor, dass sehr viele Unternehmen, gerade kleinerer Natur oder im mittelständischen Bereich, keinerlei datenschutzrechtliche Vorkehrungen getroffen haben und auch ein gewisses Grundverständnis für den Datenschutz fehlt. Das kann jedermann an kleinen Beispielen im Alltag sehen, wie z.B. in der Bahn, wo Mitreisende etwa Akten bearbeiten oder eigentlich vertrauliche geschäftliche Telefonate führen; beim Kopieren (es darf nicht passieren, dass ein kleiner Druckauftrag zwischen einem großen ausgedruckt wird oder liegenbleibt und dies später nicht heraussortiert wird) oder im Umgang mit dem Smartphone, etwa wenn Mails an Personen geschickt werden, die nicht zum eigentlich beabsichtigten Adressatenkreis gehören (etwa durch die „Autovervollständigen“-Funktion).

2. Überarbeitung der bestehenden Verträge, insb. mit Blick auf Datenschutz

Zusätzlich sollten alle bestehenden Verträge mit Blick darauf geprüft werden, ob sie den neuen Regelungen entsprechen, was nicht nur inhaltlich, sondern vor allem auch hinsichtlich der richtigen Verweise (auf die neuen Regelungen des BDSG) gilt. Hiervon sind etwa Arbeitsverträge betroffen, die üblicherweise einen Verweis auf § 5 BDSG enthalten oder Auftragsdatenverarbeitungsverträge,[33] die den neuen Anforderungen Stand halten müssen.

Schließlich gilt diese „Update“-Pflicht natürlich auch für den Franchisevertrag, wenn dieser datenschutzrechtliche Regelungen enthält. Sollte es eine entsprechende Klausel noch nicht geben, empfiehlt sich deren Aufnahme mit folgendem Mindestinhalt:[34]

---

27 Erwägungsgrund 37 lautet: „*Eine Unternehmensgruppe sollte aus einem herrschenden Unternehmen und den von diesem abhängigen Unternehmen bestehen, wobei das herrschende Unternehmen dasjenige sein sollte, das zum Beispiel aufgrund der Eigentumsverhältnisse, der finanziellen Beteiligung oder der für das Unternehmen geltenden Vorschriften oder der Befugnis, Datenschutzvorschriften umsetzen zu lassen, einen beherrschenden Einfluss auf die übrigen Unternehmen ausüben kann. Ein Unternehmen, das die Verarbeitung personenbezogener Daten in ihm angeschlossenen Unternehmen kontrolliert, sollte zusammen mit diesen als eine „Unternehmensgruppe“ betrachtet werden.*“.

28 Vgl. Art. 44 ff. DS-GVO.

29 Abgesehen von der individuell erteilten Einwilligung. Die Wirksamkeit des als Reaktion auf die EuGH-Urteile zur Europarechtswidrigkeit vereinbarten sog. „privacy shields“ ist rechtlich umstritten.

30 Vgl. anschaulich hierzu ein Interview mit *Jan Philipp Albrecht*, der als Berichterstatter und MEuP den Gesetzgebungsprozess des Europäischen Parlaments geleitet hatte, u.a. mit dem Landesdatenschutzbeauftragten von Baden-Württemberg, *Stefan Brink* sowie schließlich *Tim Wybitul*, Rechtsanwalt bei Hogan Lovells, abrufbar unter http://hoganlovells-blog.de/2017/02/01/interview-jan-albrecht-dr-stefan-brink-tim-wybitul-zum-neuen-datenschutz/#.

31 Am 9.3.2017 erfolgt eine Lesung im Bundestag; am 10.3.2017 berät der Bundesrat, der bereits sehr umfangreiche Änderungen angekündigt hat.

32 Es gilt dann vorrangig die DS-GVO und in Bereichen, in denen diese keine abschließende Regelungen enthält, das BDSG oder das entsprechende speziellere Datenschutzgesetz, wie z.B. § 11 ff. TMG.

Hinweis auf die Verarbeitung und Speicherung der Daten gem. § 4 Abs. 3 BDSG; Zustimmung des Franchisepartner zur Verwendung seiner Antrags-, Vertrags- und Leistungsdaten für Leistungsvergleiche,[35] aber auch für Markt-/Meinungsforschungs- und Werbezwecke;[36] Hinweis auf geschlossene Auftragsdatenverarbeitungsverträge mit Systemlieferanten und -dienstleistern (sowie Logistikpartnern); Ermächtigung zum Abschluss weiterer Unterauftragsdatenverarbeitungsverträgen;[37] Verpflichtung des Franchisepartners, seinerseits alle datenschutzrechtlichen Vorschriften einzuhalten gegenüber Mitarbeitern und Endkunden sowie die Erläuterung der datenschutzrechtlich relevanten Vorgänge bei der gemeinsamen Nutzung von Kassen- und IT-Systemen.[38] Häufig haben datenschutzrechtliche Einwilligungserklärungen einen Zielkonflikt zu bewältigen: Einerseits sollen sie zweckbezogen so genau wie möglich beschreiben, welchen Vorgängen der Einwilligende zustimmt und was mit seinen Daten passiert – dies führt zu langen, umständlich klingenden Bandwurmsätzen. Andererseits sollen die Klauseln aber auch transparent sowie „*verständlich und in klarer und einfacher Sprache*“ abgefasst sein,[39] was nicht immer gelingt.

3. Prüfung von besonderen Maßnahmen aufgrund der Datenschutzgrundverordnung

Besonderes Augenmerk verdient nach der DS-GVO sicherlich die Folgenabschätzung. Hier muss sorgfältig eruiert werden, inwiefern es im entsprechenden Unternehmen möglich ist, dass datenschutzrechtlich relevante Prozesse unter die Folgenabschätzung fallen.

Schließlich muss mit Blick auf die gestiegenen Sanktionsmöglichkeiten ein Prozess implementiert werden, wonach das Unternehmen regelmäßig überprüfen kann, ob es die wesentlichen datenschutzrechtlichen Vorschriften erfüllt.

IV. Fazit

Zusammenfassend ist festzustellen, dass die DS-GVO den Stellenwert des Datenschutzes deutlich heben wird[40] und sich Unternehmen ab sofort hierauf einstellen müssen – gut vierzig Jahre nach Entstehen des Datenschutzrechts ist der Datenschutz dann auch bei Unternehmen „*wachgeküsst*“ und angekommen.

Bis zum unmittelbaren Inkrafttreten im Mai 2018 müssen sowohl der Gesetzgeber, aber auch Unternehmen, ausreichend Vorsorge getroffen haben.[41] Gesetzgeber und Datenschutzaufsichtsbehörden werden bis dahin – hoffentlich – die zahlreichen noch bestehenden unklaren Regelungen näher konkretisiert haben.

Darüber hinaus wäre es wünschenswert, wenn es neben der Einhaltung der einzelnen Regelungen zu einem echten Paradigmenwechsel käme und viele Unternehmen den Datenschutz nicht mehr als lästige Bürde, sondern auch als Chance begreifen. Insofern haben die letzten Jahre übrigens durchaus gezeigt, dass datenschutzsensible Unternehmen in der öffentlichen Meinung mehr Erfolg haben als Unternehmen, die sich nach wie vor nicht darum kümmern und bei denen der Datenschutz nach wie vor im Dornröschenschlaf liegt. ■

---

33 Typischerweise werden derartige Verträge mit Dienstleistern geschlossen, wie z.B. bei der elektronischen Belegarchivierung; vgl. hierzu *Haag/Pathe*, Elektronische Belegarchivierung in Franchisesystemen, in: Jahrbuch Franchising 2016, S. 67 ff.

34 Freilich sollte hierzu bis zur Verabschiedung des DSAnpUG-EU abgewartet werden.

35 Beispiel: „*Der Franchise-Partner erklärt sein Einverständnis, dass seine personenbezogenen und betriebsbezogenen Daten anderen Partnern im Rahmen und zum Zweck von Betriebsvergleichen anonymisiert zur Verfügung gestellt werden.*“

36 Hier müssen allerdings die entsprechenden Erklärungen gem. § 4a Abs. 1 BDSG hervorgehoben sowie die Regelungen in § 7 UWG beachtet werden.

37 Beispiel: „*Der Franchise-Partner ist befugt, im vorgenannten Umfang seinerseits Unterauftragsdatenverarbeiter einzuschalten. Im Übrigen darf der Franchisegeber Unterauftragsdatenverarbeiter nur einsetzen, wenn der Franchise-Partner dem vorher zugestimmt hat. Diese Zustimmung kann auch per E-Mail oder auf sonstigem elektronischem Wege erteilt werden. Der Franchisegeber gibt an die Unterauftragsdatenverarbeiter sämtliche seiner datenschutzbezogenen Pflichten aus diesem Vertrag weiter und verpflichtet sie zudem zur Einhaltung der geltenden Datenschutzvorschriften. Um die Sicherheit der Daten des Franchise-Partners sicherzustellen, ist der Franchisegeber in derartigen Fällen verpflichtet, in den Vertrag mit den Unterauftragnehmern geeignete, den geltenden Datenschutzgesetzen entsprechende Regelungen vorzusehen und Kontrollmaßnahmen zu ergreifen und zu dokumentieren.*“

38 Beispiel: „*Die Vertragsparteien sind darüber einig, dass es für die vom Franchisegeber erbrachten Leistungen, insbesondere zur Unterstützung des Franchise-Partners durch Bereitstellung der Systemsoftware zur gemeinsamen Nutzung, die zentrale Abwicklung von Online-Bestellungen sowie ermöglichte Teilnahme des Franchise-Partners an Onlinebezahlsystemen, und in den Bereichen Kundenbetreuung, Reklamationsmanagement neben den auf den vom Franchise-Partner betriebenen Standort bezogenen Daten auch zu dem Austausch von personenbezogenen Daten der Kunden des Franchise-Partners und Interessenten an dessen Leistungen kommt.*“.

39 So Art. 7 Abs. 2 DS-GVO.

40 Vgl. *Schantz* NJW 2016, 1841: „Beginn einer neuen Zeitrechnung im Datenschutzrecht“.

41 Dies allein wird freilich nicht ausreichen: Während früher mit dem BDSG die „Dominanz des öffentlichen Rechts“ gerügt wurde, so *Büser*, a.a.O. S. 218, ist es heute viel wichtiger darauf hinzuweisen, dass nach wie vor das Recht vorgeben sollte, was erlaubt ist und nicht die Technik, die in erster Linie ihre Innovationsdynamik umsetzt und dabei von Gesetzen im Zaum gehalten werden muss, was für Gesellschaft und Gesetzgeber zunehmend eine Herkulesaufgabe darstellt, zumal im internationalen Kontext.