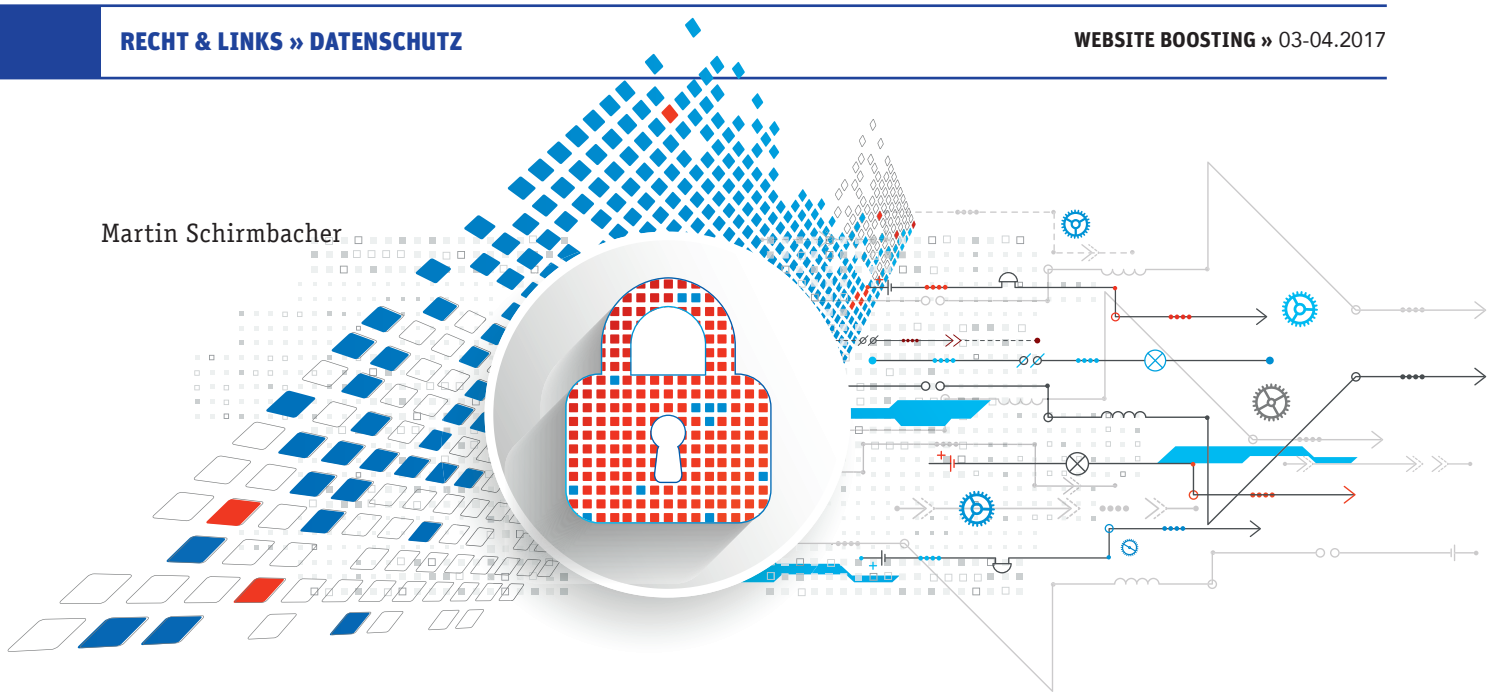
Martin Schirmbacher



Die neue Datenschutzgrundverordnung – das betrifft Sie! Was ist zu tun?

Am 25. Mai 2018 wird die neue EU-Datenschutzgrundverordnung in allen Mitgliedstaaten der Europäischen Union wirksam. Für viele Unternehmen wird sich bei der Verarbeitung personenbezogener Daten bis dahin einiges ändern müssen. Der Beitrag von Rechtsanwalt Martin Schirmbacher erläutert zunächst, was es mit der DSGVO auf sich hat und was der wesentliche Inhalt ist. Anschließend geht er für Sie auf den konkret bestehenden Umsetzungsbedarf eines Online-Unternehmens ein.

Ein wichtiges neues Gesetz im Datenschutz

Manche sagen, dass alle wichtigen Gesetze heutzutage aus Brüssel kommen. Das stimmt vielleicht nicht ganz. Für den Online-Bereich ist an dieser Aussage aber viel Wahres dran. Im besonderen Maße gilt das jedenfalls für das Datenschutzrecht. Schon lange existiert eine EU-Datenschutzrichtlinie. Ab dem nächsten Jahr wird aber eine Verordnung zu Datenschutz EU-weit gelten: die EU-Datenschutzgrundverordnung (DSGVO). Die Verordnung gilt unmittelbar in allen Mitgliedstaaten – also auch in Deutschland. Bisheriges deutsches Recht wird angepasst oder abgeschafft. Das gilt insbesondere für das Bundesdatenschutzgesetz und die Regelungen zum Datenschutzgesetz im Telemediengesetz. Beides wird es nach dem 25. Mai 2018 so nicht mehr geben.

Künftig bestimmt damit die Auslegung der Datenschutzgrundverordnung, was in Deutschland datenschutzrechtlich legal ist und was nicht. Der Text der Verordnung ist bereits beschlossen und im Amtsblatt verkündet. Der Transformationsprozess ist im vollen Gange. Insbesondere in großen Unternehmen arbeiten große Teams daran, alle Datenschutzprozesse in den Unternehmen DSGVO-compliant zu machen. Das ist auch nötig. Nach Wirksamwerden der Verordnung gibt es keine Übergangsfrist.

Ein riesiger Vorteil liegt darin, dass die DSGVO einheitliches Recht in der gesamten EU schafft. Online-Unternehmen müssen sich nur um ein Datenschutzrecht kümmern, wenn sie sich international aufstellen. Das ist jedenfalls der Grundsatz; einige Ausnahmen wird es weiterhin geben.

DER AUTOR

Dr. Martin Schirmbacher ist Fachanwalt für IT-Recht bei HÄRTING Rechtsanwälte in Berlin. Er berät Mandanten im E-Commerce, bei Softwareverträgen und im Datenschutz. Sein Buch Online-Marketing und Social-Media-Recht ist gerade in neuer Auflage erschienen.

„Neuer Wein in alten Schläuchen" oder „Alles neu macht der Mai"?

Je nachdem, auf welcher Website man Informationen zum neuen Datenschutzrecht liest, scheint mehr oder minder alles beim Alten zu bleiben oder aber tatsächlich alles neu zu sein. Die Wahrheit liegt sicher irgendwo in der Mitte und hängt auch von dem jeweiligen Blickpunkt ab. Alle deutschen Datenschützer werden umlernen müssen. Dies betrifft schon einmal die Terminologie und die Nummerierung. Hier wird in der Tat alles anders sein.

Doch auch inhaltlich gibt es viele Änderungen. Richtig ist zwar, dass der Unterschied zwischen dem geltenden Recht in anderen Mitgliedstaaten und der DSGVO deutlich größer ist. Insofern gibt es in ausländischen Unternehmen möglicherweise auch größeren Anpassungsbedarf. Doch auch deutsche Unternehmen müssen teilweise umdenken. Eine Herausforderung ist, dass sich der Verordnung vielfach die konkrete Rechtslage nicht entnehmen lässt. Das neue Gesetz ist in vielen Punkten unklar. Erst die Zeit und erste Entscheidungen von Gerichten werden zeigen, wie einzelne Regelungen jeweils auszulegen sind. Bis dahin ist vieles offen – ein sehr unbefriedigender Zustand für viele Online-Unternehmen.

Bußgelder

Fakt ist zunächst, dass für Verstöße gegen die Verordnung horrende Bußgelder drohen. Für schwere Datenschutzverstöße drohen in Zukunft 20 Millionen Euro, bei weniger schweren Verstößen bis zu 10 Millionen Euro Bußgeld. Bisher ist bei 300.000,- Euro (bzw. 50.000,- Euro) Schluss. Bei Großunternehmen kann es sogar noch deutlich darüber hinausgehen. Maximum bei schweren Verstößen ist 4 % des weltweiten Jahresumsatzes.

In welcher Höhe sich Bußgelder einpendeln werden, gehört jedoch zu den Dingen, die derzeit vollkommen offen sind. Klar ist lediglich, dass ein Bußgeld im niedrigen vierstelligen Bereich in Zukunft wohl eher nicht mehr verhängt werden wird.

Problematisch an den Bußgeldern ist nicht nur deren Höhe, sondern auch, dass die Behörden für die Frage, ob ein Bußgeld verhängt wird, nur einen sehr eingeschränkten Ermessensspeilraum haben. Wird der Datenschutzbehörde ein Datenschutzverstoß bekannt, muss dieser auch ermittelt und gegebenenfalls mit einem Bußgeld bestraft werden. Das erschwert in Zukunft eine offene Kommunikation mit den Behörden über Einzelaspekte, weil ein Behördeneinschreiten bei möglichen Datenschutzverstößen droht, die nebenbei bekannt werden.

Zwischenfazit: erhebliche Ausweitung der Bußgelder

Verarbeitung personenbezogener Daten ist verboten

Wie bisher im deutschen Recht gilt in der DSGVO das Verbotsprinzip. Das bedeutet, dass jede Art der Verarbeitung personenbezogener Daten verboten ist, es sei denn, sie ist durch ein Gesetz erlaubt oder durch eine Einwilligung gerechtfertigt.

Personenbezogen sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Das ist schon nach geltendem Recht so. Als identifizierbar gilt jeder, der direkt oder indirekt identifiziert werden kann. Dabei soll es genügen, wenn eine eindeutige Zuordnung zu Standort-Daten oder einer Online-Kennung möglich ist. Für die Identifikation soll offenbar eine Zuordnung zu einer IP-Adresse genügen. Insofern ist der Begriff des Personenbezugs nach neuem Recht eher noch weiter als nach derzeitiger Rechtslage. Ein Rückschluss auf eine konkrete natürliche Person und deren Namen ist nicht mehr erforderlich.

Vom neuen Recht betroffen ist also nicht nur jedes Unternehmen, das Arbeitnehmerdaten oder Kundendaten speichert, sondern auch alle Unternehmen, die mit IP-Adressen arbeiten – letztlich also alle Unternehmen.

Auch gilt weiterhin das Gebot der Datenminimierung, der sachlichen Richtigkeit, der begrenzten Speicherung, der Transparenz und auch der Zweckbindungsgrundsatz. Es bedarf einer erneuten Rechtfertigung, wenn Daten, die zu einem bestimmten Zweck erhoben wurden, nun zu einem anderen Zweck dienen sollen.

Zwischenfazit: Rechtslage ähnlich, IP-Adressen haben Personenbezug

Einwilligung in die Datenverarbeitung

Die Einwilligung ist bisher das wichtigste Rechtfertigungsmittel für eine Datenverarbeitung. Die gesetzlichen Regelungen für die Einwilligung sind vergleichbar, möglicherweise aber ein wenig strenger. Aufgehoben ist aber das Schriftformerfordernis. Auch elektronisch oder über ein Häkchen erteilte Einwilligungen sind ausdrücklich möglich. Einwilligungen, die in AGB eingebettet sind, müssen besonders hervorgehoben werden. Auch in Zukunft wird jede Einwilligung widerrufbar sein.

Ausdrücklich in der Verordnung steht, dass jede Einwilligung freiwillig abgegeben sein muss. Was das genau heißt, wird zu den umstrittensten Fragen der Verordnung gehören. An einer Stelle heißt es in der Verordnung, dass von Freiwilligkeit nur die Rede sein könne, wenn der Einwilligende eine echte und freie Wahl hat. Er soll die Einwilligung verweigern oder zurückzuziehen können, ohne Nachteile zu erleiden. Zum Teil wird in den Text ein sogenann-

tes Kopplungsverbot hineingelesen. Dass man einen Dienst nur nutzen kann, wenn man eine datenschutzrechtliche Einwilligung erteilt, soll in Zukunft unzulässig sein. Ob das im Ergebnis heißt, dass etwa ein werbefinanziertes News-Portal auch eine Variante ohne personalisiertes Targeting anbieten muss, ist noch offen. Ein Take-it-or-leave-it-Ansatz ist möglicherweise mit dem neuen Recht nicht vereinbar. Hier wird es einiges an Diskussionen geben.

Eine weitere Neuerung betrifft die Einwilligung von Kindern. Kinder und Jugendliche, die noch nicht 16 sind, können nur mit Zustimmung der Eltern einwilligen.

Einwilligungen, die jetzt erteilt wurden, bleiben wirksam, wenn Grundprinzipien der neuen Rechtslage eingehalten sind. Dies haben sogar die Datenschutzbehörden ausdrücklich bekundet.

Zwischenfazit: Rechtslage unklar und tendenziell eher strenger

Vertragliche Nutzung von Daten

Wie bisher auch dürfen personenbezogene Daten verwendet werden, wenn dies für die Erfüllung eines Vertrages erforderlich ist. So dürfen etwa die Adressdaten einer Person gespeichert werden, um dort Waren auszuliefern. Auch die Weitergabe von Daten an ein Inkassounternehmen oder einen Anwalt zur Beitreibung von Forderungen ist legitim.

Zwischenfazit: Rechtslage identisch

Rechtfertigung mit berechtigten Unternehmensinteressen

Die wichtigste Vorschrift in der DSGVO ist einigermaßen versteckt. In Artikel 6 Absatz 1 Buchstabe f) gibt es einen Passus, wonach auch ein berechtigtes Interesse des datenverarbeitenden Unternehmens in bestimmten Fällen die Datenverarbeitung rechtfertigen kann. Erforderlich ist ein berechtigtes Interesse und dass die Datenverarbeitung zur Erreichung dieses Interesses notwendig ist. Außerdem dürfen schutzwürdige Interessen des Betroffenen nicht überwiegen.

Nötig ist also ein berechtigtes Interesse, wobei jedes von der Rechtsordnung gebilligte (auch wirtschaftliche) Interesse genügt. Die Datenverarbeitung muss notwendig sein. Es darf also keinen anderen zumutbaren Weg geben, das gewünschte Ergebnis zu erreichen, bei dem weniger stark in das Datenschutzrecht eingegriffen wird. Kann etwa ein bestimmtes Ziel auch beim Arbeiten mit Pseudonymen erreicht werden, sollten auch Pseudonyme eingesetzt werden. Außerdem muss man eine Abwägung der beteiligten Interessen vornehmen. Dabei kommt es auf die vernünftigen Erwartungen der Betroffenen an. Ein Nutzer, der in einer konkreten Situation die Verarbeitung seiner Daten erwarten kann, ist weniger schutzwürdig, als wenn er damit nicht rechnen muss. In der Verordnung selbst steht, dass auch die Direktwerbung ein berechtigtes Interesse sein kann.

Im Bereich der berechtigten Interessen ist noch vieles unklar. Es sieht so aus, als gäbe es hier gewisse Spielräume für Unternehmen. Diese Spielräume gilt es zu nutzen. Dazu ist aber jeweils eine Prüfung des neuen Rechts im Einzelfall nötig.

Zwischenfazit: Rechtslage möglicherweise unternehmensfreundlicher

Neue Pflicht: Opt-out-Möglichkeit bei der Direktwerbung

Wichtig ist, dass für jede Maßnahme der Direktwerbung eine Opt-out-Möglichkeit implementiert wird. Der Nutzer hat jederzeit das Recht, Widerspruch gegen die Verarbeitung seiner personenbezogenen Daten zum Zwecke der Direktwerbung einzulegen. Darüber muss der Nutzer auch jeweils in transparenter Weise unterrichtet werden. Dies geschieht üblicherweise in einer transparenten Datenschutzerklärung auf der Website. Diese Datenschutzerklärungen sind an das neue Recht anzupassen. Es gibt auch neue Informationspflichten, die man beachten muss.

Zwischenfazit: Neues Pflicht-opt-out für jede Datenverarbeitung zum Zwecke der Direktwerbung

Compliance, Compliance, Compliance ...

Die DSGVO enthält wie schon geltendes Recht die Pflicht, ein Verfahrensverzeichnis zu führen. Zwar gibt es Ausnahmen für Unternehmen mit weniger als 250 Mitarbeitern. Verfahren, die nicht nur gelegentlich angewendet werden, müssen jedoch im Verzeichnis auftauchen. Ob das dauerhafte Tracking oder Targeting von Nutzern darunter fällt, ist offen.

Ein erhebliches Compliance-Risiko bildet die Anforderung, vorab eine Datenschutz-Folgenabschätzung vorzunehmen. Dies gilt insbesondere bei der Profilbildung. Auch, wann genau eine Profilbildung vorliegt, ist noch nicht klar. Die Folgenabschätzung ist letztlich eine detaillierte Beschreibung des geplanten Verarbeitungsverfahrens, die auch eine Bewertung der Notwendigkeiten und Verhältnismäßigkeiten der Datenverarbeitung beinhaltet. Auch Schutzmaßnahmen und Sicherheitsvorkehrungen müssen im Detail beschrieben werden.

Wer sich nicht an die Vorgaben hält, handelt ordnungswidrig und Bußgelder drohen. Das gibt den Beratern

einen Packen an Hausaufgaben, der im Laufe der nächsten Monate erledigt werden muss.

Zwischenfazit: Rechtslage wird strenger

Fazit zum Inhalt der Verordnung

Auch wenn die DSGVO von den Grundprinzipien her durchaus mit dem BDSG vergleichbar ist, gibt es doch gravierende Änderungen. Die Compliance-Anforderungen sind deutlich höher. Ob einzelne Datenverarbeitungsmethoden weiterhin zulässig sind, muss man im Detail prüfen. Datenschutzrechtliche Texte (Einwilligung, Datenschutzerklärung) müssen überarbeitet werden. Und das Ganze ist keine Lappalie. Jedenfalls der neue Bußgeldrahmen sorgt für erheblichen Anpassungsdruck bei den Unternehmen. Insofern macht der Mai 2018 vielleicht nicht alles neu, der Wein, der durch die Schläuche fließt, ist aber definitiv frisch. Ob er schmeckt, muss jedes Unternehmen für sich beantworten.

Unternehmen müssen jetzt tätig werden

Die landläufige Meinung scheint derzeit zu sein, dass man noch abwarten könne. Es sei ja schließlich noch mehr als ein Jahr Zeit, bis die Verordnung wirklich gilt. Nach aktuellen Studien von Wirtschaftsverbänden haben sich mehr als die Hälfte der deutschen Unternehmen mit dem Thema überhaupt noch nicht befasst. Das ist leider ein Irrglaube. Auch in kleineren Unternehmen kann sich ein DSGVO-Projekt schnell auswachsen. Nicht nur Banken, Versicherungen und große Konzerne müssen sich kümmern. Auch kleinere Unternehmen und Start-ups müssen dem Thema schnell ein Mindestmaß an Aufmerksamkeit widmen.

NEUN FRAGEN ZUR DATENSCHUTZGRUNDVERORDNUNG

1. Wir sind im Datenschutz eigentlich ganz gut aufgestellt, betrifft uns die DSGVO?
Ja! Jedes Unternehmen, das personenbezogene Daten speichert oder nutzt, muss sich um das neue Recht kümmern.

2. Ich denke, die Verordnung gilt erst im nächsten Jahr, müssen wir uns jetzt schon kümmern?
Ja! Jedenfalls Einwilligungserklärungen, ADV-Vereinbarungen und Datenschutzerklärung sollten jetzt schon angepasst werden. Außerdem müssen alle datenschutzrechtlich relevanten Prozesse einmal auf den Prüfstand.

3. Was ist denn die krasseste Änderung?
Die deutlichste Änderung ist sicher der Bußgeldrahmen. Bis zu 20 Millionen Euro oder 4 % vom weltweiten Jahresumsatz können Datenschutzverstöße in Zukunft kosten.

4. Und inhaltlich?
Da ist für jeden etwas dabei. IP-Daten werden in Zukunft wohl eindeutig zu den personenbezogenen Daten zählen, sodass jede Erhebung rechtfertigungsbedürftig ist. Die Anforderungen an die Einwilligung des Nutzers werden eher steigen.

5. Gibt es auch positive Dinge?
Die Verordnung an sich ist schon einmal ein Fortschritt: Grundsätzlich gilt nun einheitliches Datenschutzrecht in der ganzen EU. Aber auch sonst gibt es einige Bereiche, wo das neue Recht weniger streng zu sein scheint, als das BDSG. So lassen sich Datenverarbeitungsvorgänge mit berechtigten Interessen des Unternehmens rechtfertigen. Ausdrücklich nennt die Verordnung die Direktwerbung als berechtigtes Interesse.

6. Was gibt es sonst noch Neues?
Vor allem Compliance-Anforderungen: ein Datenschutzkonzept und Datenschutzfolgeabschätzungen. Alles eher Fleißarbeit als Rocket-Science, aber wichtig.

7. Wer sollte sich kümmern?
Datenschutz sollte jedenfalls zeitweise Chefsache sein. CEO oder Geschäftsführer muss sich davon überzeugen, dass das Unternehmen für 2018 gut aufgestellt ist und alle Hausaufgaben angegangen werden.

8. Brauchen wir externe Unterstützung?
Ein DSGVO-Projekt braucht Datenschutz-Know-how, das in vielen Unternehmen nicht oder nicht in ausreichendem Umfang vorhanden ist. Für die meisten Unternehmen wird es sich auch nicht lohnen, temporär Know-how aufzubauen. Außerdem sind gute Datenschützer zurzeit rar. Daher wird es ohne externe Unterstützung nicht gehen.

9. Was kostet so ein DSGVO-Projekt?
Das lässt sich seriös nicht beziffern und hängt von vielen Faktoren ab. Hauptkriterium ist sicher, wie gut das Unternehmen schon bisher datenschutzrechtlich aufgestellt ist. Wenn es bisher nicht einmal ein Verfahrensverzeichnis und einen vernünftigen Prozess zur Beantwortung eines Auskunftsersuchens gibt, ist das mehr Aufwand, als wenn der bisherige Datenschutzbeauftragte es insofern genau genommen hat. Führt ein Assessment dazu, dass IT-Infrastruktur konzernweit angepasst werden muss, ist offensichtlich, dass es mit ein paar Meetings und ein bisschen Paperwork nicht getan ist. Insofern geht die Spanne bei ein paar Tausend Euro los und ist nach oben offen.

Die Eilbedürftigkeit folgt zum einen daraus, dass ein gutes Jahr für die Umsetzung eines solchen Projektes nicht viel ist. Das gilt vor allem, wenn einzelne Prozesse oder IT-Infrastruktur umgestellt werden müssen. Ergibt eine Prüfung nach neuem Recht beispielsweise, dass ein neues Berechtigungskonzept geschaffen werden muss, lässt sich das kaum in wenigen Wochen umsetzen.

Vor allem aber müssen jetzt schon Weichen für spätere Compliance gestellt werden. Zwar meinen auch die Datenschutzbehörden, dass alte Einwilligungen gültig bleiben. Doch soll dies nur gelten, wenn die Bedingungen der DSGVO im Wesentlichen eingehalten werden. Dazu gehört nach Ansicht der Datenschützer vor allem, dass das Kopplungsverbot beachtet wird. Wer also sichergehen will, dass heute eingeholte Einwilligungen auch nach dem 25. Mai nächsten Jahres noch belastbar sind, muss heute schon die Reichweite des neuen Kopplungsverbots prüfen und entsprechend handeln. Auch Datenschutzerklärungen sollten schon jetzt angepasst werden, damit eine zukünftige Nutzung der Daten ohne Weiteres möglich ist.

Ein kleines DSGVO-Projekt

Große Unternehmen arbeiten schon seit Monaten, manche seit Jahren, an DSGVO-Projekten. Doch auch der Mittelstand und kleinere Unternehmen der Online-Branche müssen nun aufwachen und schon angesichts der Bußgelder das neue Datenschutzrecht in Angriff nehmen. Unterscheiden kann man dabei drei Bereiche:

(1) Status quo: Aufstellung und Prüfung der Datenverarbeitungsvorgänge im Unternehmen

Existiert ein Verfahrensverzeichnis, kann dieses herangezogen werden. Anderenfalls muss ein solches erstellt werden. Die DSGVO verlangt eine solche Aufstellung ohnehin. Anschließend sollte eine GAP-Analyse vorgenommen werden. Welche Verarbeitungsvorgänge gibt es, bei denen nach neuem Recht keine hinreichende Rechtfertigung besteht? Anschließend müssen bestehende Lücken durch Änderungen der Verfahrensweise oder zusätzliche Rechtfertigungsgründe geschlossen werden.

(2) Anpassung der Datenschutztexte

Alle Dokumente mit Datenschutzbezug und Außenwirkung müssen geprüft und gegebenenfalls angepasst werden. Zunächst sind also alle datenschutzrechtlich relevanten Dokumente zusammenzutragen. Dazu zählen insbesondere Einwilligungen, Nutzungsbedingungen und AGB, aber auch alle Verträge mit Dienstleistern und Lieferanten, zum Beispiel Auftragsdatenverarbeitungsverträge. Anschließend müssen diese angepasst werden.

(3) Datenschutzkonzept: Sicherstellung von Compliance im Unternehmen

Deutlich wichtiger als bisher werden Compliance-Anforderungen sein. Hier geht es vor allem darum, Strukturen zu schaffen, die hohe Datenschutzstandards im Unternehmen gewährleisten. Die DSGVO sieht hier verschiedene Mechanismen vor. Dazu zählen vor allem die Datenschutzfolgeabschätzung und ein Datensicherheitskonzept. Auch ein Datenschutzbeauftragter muss nach neuem Recht grundsätzlich bestellt werden. Möglicherweise wird die hierfür geltende Grenze von 20 Mitarbeitern deutlich angehoben.

Das neue Recht sieht vor, dass jedes Unternehmen über die Einhaltung der Standards jederzeit Rechenschaft ablegen können muss. Auch hierfür sind Vorbereitungen zu treffen. Die kleinste, aber sicher nicht unwichtigste Aufgabe ist, festzulegen, wer dafür verantwortlich sein soll.

Schon bisher muss jedes Unternehmen Auskunft über alle gespeicherten Daten erteilen, wenn ein Betroffener dies wünscht. Die DSGVO sollten alle Unternehmen, denen ein jedes Auskunftsersuchen bisher immer Schweißausbrüche oder Kopfzerbrechen bereitet hat, nutzen, um einen vernünftigen handhabbaren Prozess aufzusetzen.

Fazit

Das Ganze hört sich nach einigem Aufwand an. Und leider ist das auch so. Doch der Aufwand wird nicht dadurch weniger werden, dass man ihn verschiebt. Datenschutz sollte spätestens mit den neuen Bußgeldmöglichkeiten der Behörden Chefsache im Unternehmen sein. Wen der Datenschutzbeauftragte bisher nicht auf die DSGVO angesprochen und um ein Budget gebeten hat, sollte sich nun – selbst – kümmern und zunächst ein kleines Projekt aufsetzen. ¶