EU-DSGVO 2018

NUR NOCH NEUN MONATE BIS ZUR DATENSCHUTZ-RECHTLICHEN ZEITENWENDE

Die Übergangsphase zum Inkrafttreten der europäischen Datenschutzgrundverordnung (EU-DSGVO) läuft auch für Verbände

Das Datenschutzrecht wird am 25. Mai 2018 mit einer vollkommenen Veränderung der gesetzgeberischen Landschaft gänzlich neue Anforderungen an die Verantwortlichen in Verbänden stellen. War bislang das nationale Datenschutzrecht im Bundesdatenschutzgesetz für die privatrechtlichen Verbände (Berufs- und Wirtschaftsverbände) bzw. in den Landesdatenschutzgesetzen für die öffentlich-rechtlichen Verbände (Kammern) vielfach als eine Art „Papiertiger" empfunden worden, ändert sich dies im kommenden Jahr massiv. Datenschutz ist künftig Kernelement der Verbandscompliance! Was ändert sich, was bleibt gleich?

Ralf Wickert

Bislang galt in der Praxis oft die Aussage, man müsse sich dieses Themas nur dann annehmen, wenn man im Rahmen einer aufsichtsrechtlichen Überprüfung oder eines kleineren Bußgeldbescheides hierzu angehalten werde. Die Aufsichtsbehörden selbst hatten gar nicht die personellen Kapazitäten, für eine wirksame Durchsetzung datenschutzrechtlicher Anforderungen zu sorgen.

Dies wird sich am 25. Mai 2018 massiv ändern, da dann die Europäische Datenschutz Grundverordnung unmittelbar auch in Deutschland gilt und weiterhin am gleichen Tag das kürzlich am 30. Juni 2017 beschlossene neue Bundesdatenschutzgesetz (Bundesgesetzblatt I 2017, Seite 2097 ff.) in Kraft tritt. Zwar werden die wesentlichen und schon im heutigen Recht tragenden Prinzipien des Datenschutzes, nämlich insbesondere des sogenannten Verbotes mit Erlaubnisvorbehalt, beibehalten, es gibt aber massive Veränderungen und einen erheblich ausgeweiteten Bußgeldrahmen, der dem politisch gewollten effektiven Datenschutz Rechnung trägt.

Nach der Grundverordnung können künftig Bußgelder bis zu 20 Millionen Euro oder bei Unternehmen vier Prozent des Konzernumsatzes erhoben werden, sodass die Bebußung kartellrechtliche Ausmaße erreicht und mithin auch kleinere Verstöße ganz erhebliche bußgeldrechtliche Folgen nach sich ziehen.

MEHR KONTROLLEN

Weiterhin haben die Aufsichtsbehörden angekündigt, ihre personellen Kapazitäten so auszuweiten, dass effektiver Datenschutz auch kontrolliert werden kann und mithin rein situatives Eingreifen der Aufsichtsbehörden im Einzelfall etwa auf die Anzeige eines Verbandsmitgliedes hin der systematischen Kontrolle weichen wird.

Nachfolgend soll rechtzeitig vor Mai 2018 ein Überblick über Kernelemente der Grundverordnung gegeben werden, damit die Verbände rechtzeitig die erforderlichen Maßnahmen ergreifen können, um nicht erst nach einem möglicherweise drakonischen Bußgeld wach zu werden.

ZUNÄCHST DAS ZENTRALE KONZEPT DER DATENVERARBEITUNG

Auch in Zukunft ist die Verarbeitung von Daten, die Rückschlüsse auf eine Person zulassen, nur dann möglich, wenn entweder die betroffene Person eingewilligt hat oder eine der weiteren in Art. 6 Abs. 1 der Datenschutz-Grundverordnung benannten Rechtsgrundlagen für eine Datenverarbeitung greifen:

- Erfüllung eines Vertrages bzw. Anbahnung eines Vertrages auf Veranlassung des Betroffenen;
- rechtliche Verpflichtung des Verantwortlichen, also des Verbandes;
- lebenswichtige Interessen einer Person;
- Wahrnehmung einer Aufgabe im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt oder
- überwiegende Interessen des Verantwortlichen oder eines Dritten.

Dies sind im Kern die systematischen Voraussetzungen für eine Datenverarbeitung, die heute schon gelten und in § 4 Abs. 1 BDSG auch so benannt sind.

Neben diesem Grundsatz der rechtmäßigen Datenverarbeitung, die ihre Zwecke dem Betroffenen immer offenlegen muss, und einer Stärkung des Prinzips der Datensparsamkeit ist insbesondere das Prinzip der Transparenz und Integrität sowie Vertraulichkeit hinzugekommen. Weiterhin gibt es erhebliche Ausweitungen der Rechenschaftspflicht der Verantwortlichen, die bei den Verbänden organisatorisch Maßnahmen fordern, um dieser Rechenschaftspflicht zu genügen.

ERWEITERUNGEN BEI DEN AUSKUNFTSRECHTEN VON BETROFFENEN

Schon im bisherigen Recht gab § 34 BDSG den Betroffenen ein Auskunftsrecht, mit dem sie bei den verantwortlichen Stellen, also den Verbänden, gezielt über die dort gespeicherten personenbezogenen Daten Informationen verlangen konnten. Dieses Recht wird durch Art. 15 Abs. 1 der Grundverordnung erheblich gestärkt, da die Grundverordnung jetzt den Katalog der Informationen zwingend vorgibt, die den Betroffenen mitzuteilen sind.

Nach Art. 15 Abs. 1 muss der Verband als Verantwortlicher folgende Informationen mitteilen:

- Er muss zunächst sagen, ob bei ihm personenbezogene Daten verarbeitet werden, und wenn ja, welche Daten dies genau sind.
- Weiter muss er die Verarbeitungszwecke nennen und die Kategorien der personenbezogenen Daten aufzeigen. Diese Anforderung ist neu.
- Sodann muss er die möglichen Datenempfänger benennen.
- Er muss die Speicherdauer, die er plant, bezeichnen können, eine Anforderung, die bislang nicht im Gesetz enthalten war. Eine geplante Speicherdauer kann nur derjenige Verband effektiv mitteilen, der ein ausreichendes Löschungskonzept hat, aus dem die zeitlichen Zielsetzungen hinsichtlich der Speicherung bzw. Löschung personenbezogener Daten hervorgehen.
- Er muss Informationen über Rechte auf Berichtigung, Löschung, Einschränkung der Verarbeitung sowie ein Widerspruchsrecht nach Art. 21 der Grundverordnung erteilen, was ebenfalls im Bundesdatenschutzgesetz so nicht vorgesehen war.
- Neu ist auch die zwingende Information über das Beschwerderecht bei der Aufsichtsbehörde.
- Die Information hat weiterhin die Herkunft oder Quelle der Daten offenzulegen, soweit diese – was häufig der Fall sein wird – nicht bei der betroffenen Person selbst erhoben worden.
- Letztlich muss der Verband über das Bestehen einer automatisierten Entscheidungsfindung und ein sogenanntes Profiling informieren, was ebenfalls eine neue Anforderung ist.

Diese Informationen sind dem Betroffenen schriftlich, elektronisch oder mündlich zu erteilen, möglichst in Form einer Kopie (Art. 15 Abs. 3 der Grundverordnung). Hier stellt sich der europäische Gesetzgeber im Idealzustand einen Fernzugriff der betroffenen Person über die Daten vor, die der Verband über ihn vorhält. Der Verband muss nämlich die Informationen in einem „gängigen elektronischen Format“ zur Verfügung stellen, wenn die Anfrage an ihn elektronisch gerichtet wird. Hieraus ergeben sich erhebliche Anforderungen an die Automatisierungsprozesse in der Datenverarbeitung, da insbesondere in Massenprozessen, wie dies bei mitgliederstarken Berufsverbänden eigentlich üblich ist, eine Informationspflicht innerhalb der Frist von einem Monat, den die Grundverordnung in Art. 12 Abs. 3 vorgibt, nur dann erfüllt werden kann, wenn praktisch vorsorglich alle Maßnahmen ergriffen werden, im Bedarfsfalle auch informieren zu können. Man denke etwa an einen Berufsverband mit mehreren 10.000 Mitgliedern und die dortigen Verarbeitungsprozesse der berufsangehörigen Mitglieder. Wenn sich der Verband hier nicht organisatorisch auf die Erfüllung solch strenger Informationsrechte von vorneherein einstellt, läuft er Gefahr, im Bedarfsfalle die Informationen nicht rechtzeitig erteilen zu können, was dann wieder bußgeldbewehrt ist.

DOKUMENTATIONSPFLICHT ÜBER VERARBEITUNGSPROZESSE?

Das bisherige öffentliche Verfahrensverzeichnis und die interne Verarbeitungsübersicht gemäß § 4 Buchst. g Abs. 2 und Abs. 2 Buchst. a BDSG werden abgelöst durch ein Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 Abs. 5 der Grundverordnung, die aber grundsätzlich nur diejenigen Organisationen zwingend zu erfüllen haben, die mindestens 250 Mitarbeiter beschäftigen. Dies dürfte also von der formalen Seite nur die größeren Verbände treffen, es sei denn, besondere Datenkategorien gemäß Art. 9 Abs. 1 der Grundverordnung werden nicht nur gelegentlich verarbeitet, was etwa Gesundheitsdaten oder die Gewerkschaftszugehörigkeit sind. Dies könnte etwa im Zusammenhang mit der Lohnbuchhaltung zu Dokumentationspflichten führen, die auch kleinere Verbände trifft.

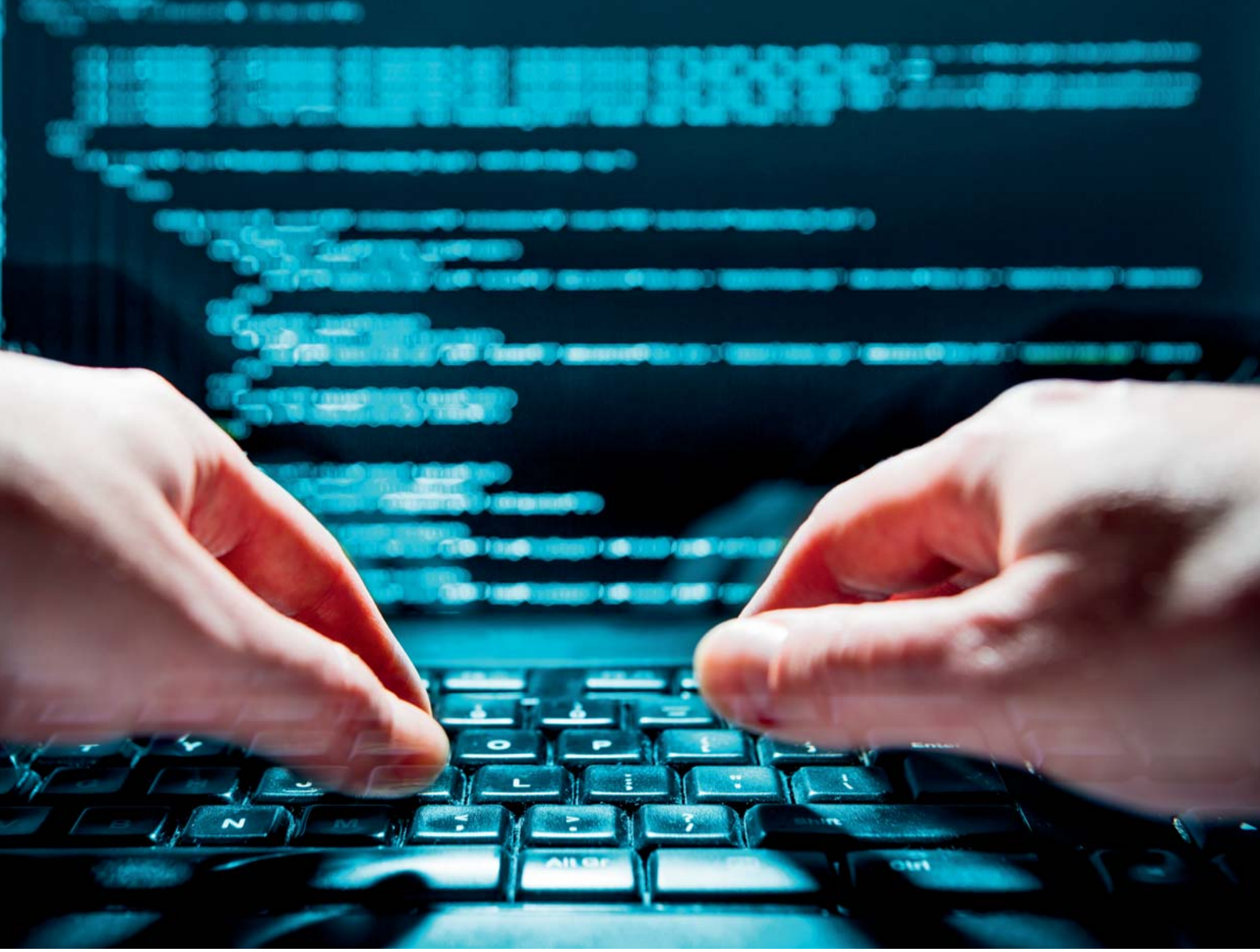
Von daher sollten die Verbände im Rahmen ihrer Maßnahmen zur Vorbereitung auf die Einführung der Grundverordnung zwingend überprüfen, ob sie ein solches Verzeichnis von Verarbeitungstätigkeiten führen müssen oder nicht.

HORRORSZENARIO DATENPANNE

Ein wesentliches Vollzugsproblem effektiven Datenschutzes sind die bislang hohen Hürden, die nach § 42a Bundesdatenschutzgesetz an die Meldepflicht von sogenannten Datenpannen knüpfen. Die jährliche Gesamtzahl solcher Meldungen von Datenpannen soll sich in der Vergangenheit bei zweistelligen Meldungen pro Jahr in Deutschland bemessen. Diese niedrige Zahl hängt – neben einer anzunehmenden hohen Dunkelziffer – wesentlich damit zusammen, dass nur dann eine Meldepflicht bestand, wenn besondere Kategorien von Daten im Rahmen der Datenpanne betroffen waren oder schwerwiegende Beeinträchtigungen drohten.

Diese hohen Hürden senkt die Grundverordnung in den Artikeln 33 und 34 deutlich ab. Das Regel-Ausnahme-Prinzip wird umgekehrt!

Eine Meldung einer Datenpanne darf nur dann unterbleiben, wenn diese „voraussichtlich nicht zu einem Risiko“ für den Betroffenen führt. Da bei den meisten Datenpannen überhaupt nicht abgeschätzt werden kann, welche Risiken drohen, führt dies faktisch zu einer Meldepflicht. Die betroffenen Personen müssen nur informiert werden, wenn ein hohes Risiko für ihre Rechte und Freiheiten besteht. Liegt eine Meldepflicht vor, so muss diese innerhalb von 72 Stunden erfüllt werden. Man denke einmal an den praktischen Fall, in dem EDV-Anlagen eines Verbandes gehackt oder sonst Daten gestohlen werden oder abhandenkommen.



WENN SICH DER VERBAND HIER NICHT ORGANISATORISCH AUF DIE ERFÜLLUNG SOLCH STRENGER INFORMATIONSRECHTE VON VORNEHEREIN EINSTELLT, LÄUFT ER GEFAHR, IM BEDARFSFALLE DIE INFORMATIONEN NICHT RECHTZEITIG ERTEILEN ZU KÖNNEN, WAS DANN WIEDER BUSSGELDBEWEHRT IST.

Liegt diese Situation vor, kann doch bei Lichte betrachtet überhaupt nicht eingeschätzt werden, was mit den Daten passiert, da man ja noch nicht einmal weiß, wer jetzt über die Daten verfügt und welche Intentionen derjenige hegt.

Von daher werden Meldepflichten bei Datenpannen erheblich relevanter als in der Vergangenheit und lösen in aller Regel eine Meldepflicht bei der Aufsichtsbehörde aus, die dann ihrerseits – und hier muss man kein Prophet sein – eine Überprüfung der datenschutzrechtlichen Situation im Verband und hier insbesondere der getroffenen technischen und organisatorischen Maßnahmen zum Schutz der personenbezogenen Daten nach sich ziehen wird. Wenn dann festgestellt wird, dass die Datenpanne letztlich Ausfluss eines generell unzureichenden Schutzniveaus ist, drohen hohe Bußgelder. Bei der Bemessung des Bußgeldes ist es nämlich nach Art. 83 Abs. 2 lit. c der Grundverordnung so, dass die Maßnahmen zur Minderung eines entstehenden Schadens Einfluss auf die Höhe des Bußgeldes haben werden. Damit kann nur der Verband damit rechnen, (noch) akzeptable Bußgelder zu erzielen, der grundsätzlich die Anforderungen des Datenschutzrechts erfüllt und bei dem sich in Gestalt der Datenpannen nur ein unerkanntes Risiko realisiert hat.

Die bisherige Limitierung der Meldepflicht auf Fälle, in denen Bank- oder Gesundheitsdaten betroffen waren, gehört jedenfalls der Vergangenheit an.

VERBÄNDE SOLLTEN IM RAHMEN IHRER MASSNAHMEN ZUR VORBEREITUNG AUF DIE EINFÜHRUNG DER GRUNDVERORDNUNG ZWINGEND ÜBERPRÜFEN, OB SIE EIN SOLCHES VERZEICHNIS VON VERARBEITUNGSTÄTIGKEITEN FÜHREN MÜSSEN ODER NICHT.

WER IST FÜR DIESE GANZEN MASSNAHMEN VERANTWORTLICH?

Hier bleibt es dabei, dass naturgemäß die Organe eines Verbandes, in aller Regel also ehrenamtliche Vorstände, für die Einhaltung des Datenschutzrechtes verantwortlich sind. Da es jedoch im Ehrenamt von Ausnahmen abgesehen kaum realistisch sein wird, effektiven Datenschutz selbst zu gewährleisten, wird man in ganz erheblichem Maße auf den Sachverstand der eigenen Organisation und hier naturgemäß auch des Datenschutzbeauftragten angewiesen sein.

Liest man nur die Grundverordnung, so wären die allermeisten Verbände von der Verpflichtung zur Bestellung eines Datenschutzbeauftragten befreit. Art. 37 der Grundverordnung gibt eine solche Verpflichtung nämlich eigentlich nur Behörden und öffentlichen Stellen sowie Organisationen auf, deren Kerntätigkeit in der systematischen Überwachung von Personen liegt (z. B. Auskunfteien) oder deren Kerntätigkeit in der Verarbeitung besonderer Kategorien von Daten (z. B. Gesundheitsdaten, Religionsdaten oder die Gewerkschaftszugehörigkeit) besteht.

Hier hat jedoch Deutschland im neuen Bundesdatenschutzgesetz eine Sonderregelung getroffen. Grundlage dieser Bestimmung im neuen Bundesdatenschutzgesetz ist eine spezielle Öffnungsklausel in Art. 37 Absatz 4 die Regelungen für nationale Bestimmungen vorhält. Allerdings gilt der Grundsatz, dass die Grundverordnung eine Art Mindestschutz gewährleisten soll und mithin Verschärfungen der Grundverordnung (selbstverständlich) weiterhin erlaubt sind. Deshalb hat sich der deutsche Gesetzgeber dafür entschieden, in § 38 BDSG-neu das bisherige Konzept der Verpflichtung zur Bestellung eines Datenschutzbeauftragten beizubehalten, sodass auch künftig Verbände immer dann einen internen oder externen Datenschutzbeauftragten bestellen müssen, wenn mindestens zehn Personen ständig mit der automatisierten Verarbeitung von personenbezogenen Daten beschäftigt sind. Schon bislang führte dies mit Ausnahme kleinerer Organisationen fast immer zu einer Bestellungspflicht, da neben den Mitarbeitern auf der Verbandsgeschäftsstelle hier auch alle ehrenamtlichen Funktionsträger des Verbandes mitzählen, solange sie in die automatisierte Verarbeitung eingebunden sind, was heute praktisch aufgrund des technischen Standes immer der Fall sein wird.

Wird entgegen einer gesetzlichen Verpflichtung ein Datenschutzbeauftragter nicht bestellt, so droht eine empfindliche Geldbuße.

NEU IST DAS EXPLIZITE RECHT AUF VERGESSENWERDEN

Das Recht auf Vergessenwerden, welches teilweise auch als „digitaler Radiergummi“ verstanden wird, ist letzt-

Externe Dienstleister sind bei der Erarbeitung eines Datenschutzmanagementsystems (DMS) zu berücksichtigen!

lich eine Folge der Rechtsprechung des Europäischen Gerichtshofs in der Entscheidung „Google Spain“ vom 13. Mai 2014 (Aktenzeichen C 131/12). Schon in dieser Grundsatzentscheidung stärkte der EuGH die Rechte der Betroffenen gegenüber Suchmaschinen erheblich und räumte diesen ein Recht auf Vergessenwerden im Internet ein. Bei Lichte betrachtet stellt dieses Recht nicht wirklich etwas Neues dar, da schon das Bundesdatenschutzgesetz erhebliche Löschungstatbestände vorgesehen hatte. Art. 17 Abs. 1 der Grundverordnung räumt den Betroffenen ein allgemeines Löschungsrecht insbesondere dann ein, wenn der Zweck der Datenverarbeitung weggefallen ist oder die Einwilligung widerrufen wird.

Neu ist jetzt, dass derjenige, der die Daten öffentlich gemacht hat – etwa im Internet –, nicht nur zur eigenen Datenlöschung verpflichtet ist, sondern auch Dritte über die Löschungspflichten zu informieren hat. Für Verbände bedeutet dies, dass die häufig beabsichtigte weite Streuung der Aktivitäten im Internet organisatorisch kontrolliert werden muss, da man von vorneherein angemessene Maßnahmen zu treffen hat, um andere Verantwortliche, die über die Aktivitäten ebenfalls im Netz berichten, über Löschungstatbestände zu informieren.

Solche Aspekte gewinnen etwa an Bedeutung, wenn das bei Verbänden gerne praktizierte Veröffentlichen von Mitgliederlisten im Netz fortgeführt wird. Die Wirtschaftsverbände können sich dieser Problematik schon dadurch entziehen, dass sie letztlich nur über den Rechtsträger, nicht jedoch dort verantwortliche Personen ihres Mitgliederkreises informieren. Dann liegen schon gar keine

personenbezogenen Daten vor, sodass sich die Diskussion der Anwendbarkeit datenschutzrechtlicher Grundsätze insoweit erledigt. Bei den Berufsverbänden wird man hier künftig viel vorsichtiger sein müssen, da es schon fraglich sein dürfte, ob Mitgliederdaten im Netz bei der nach Art. 6 Abs. 1 lit. f in der Regel vorzunehmenden Abwägung überhaupt veröffentlicht werden dürfen. Wenn dann noch das Recht auf Vergessenwerden bei etwaiger Publizierung solcher Listen hinzukommt, sollte man sich künftig die Veröffentlichung von Mitgliederlisten gut überlegen.

DIE MITNAHME VON DATEN

Art. 20 Abs. 1 der Grundverordnung gibt dem Betroffenen künftig das Recht, die eigenen personenbezogenen Daten, die zur Verfügung gestellt wurden, in einem „strukturierten, gängigen und maschinenlesbaren" Format vom Verband als Verantwortlichem zu erhalten. Ziel ist es, eine sogenannte Datenportabilität zu erreichen, um Profile und Bilder mitnehmen zu können. Dies betrifft zwar in erster Linie soziale Netzwerke, kann jedoch auch für Verbände von Bedeutung sein, wenn diese etwa Blogs und Mitglieder-Chats vorhalten, die dann reproduzierbar sein müssen.

TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN

Die Anlage zu § 9 BDSG sieht im bisherigen Recht verschiedene Maßnahmen vor, die eine verantwortliche Stelle ergreifen muss, um die Datensicherheit zu erhöhen. Hierzu zählen etwa eine effektive Zutrittskontrolle sowie ein Passwortschutz und die Verpflichtung zur Erstellung von Sicherungskopien. Auch die Grundverordnung hat die Datensicherheit im Fokus. Dem trägt Art. 32 Rechnung, indem er der Sicherheit der Verarbeitung eine besondere Bedeutung beimisst, wobei sie jedoch nicht entsprechend den Bestimmungen im Bundesdatenschutzgesetz explizit beschreibt, welche technischen und organisatorischen Maßnahmen zu wählen sind, um ein solches angemessenes Schutzniveau abzusichern. Den Verbänden als Verantwortliche ist in der Übergangsphase dazu zu raten, die bisherigen Maßnahmen fortzuführen und an den Stand der Technik, der in der Datenschutz-Grundverordnung praktisch permanent gewahrt sein muss, anzupassen.

Insgesamt ist die Datenschutz Grundverordnung techniklastiger als das Bundesdatenschutzgesetz. So greift Art. 25 der Grundverordnung das Konzept des Datenschutzes durch Technik (pricvacy by design) und der Nutzung datenschutzfreundlicher Voreinstellungen (privacy by default) auf. Hieraus folgt, dass die Verbände im Bereich des Einsatzes technischer Mittel die Verarbeitung stets so einzurichten haben, dass die Einhaltung der Grundsätze der Datenschutz-Grundverordnung gewährleistet ist. Sie müssen insbesondere Voreinstellungen im Netz so einrichten, dass die Daten nur für den jeweiligen Zweck verarbeitet werden dürfen, was in der Praxis noch so manche Schwierigkeit mit sich bringen wird.

Des Weiteren verlangt Art. 32 Abs. 1 eine Risikobewertung, unter deren Berücksichtigung die Maßnahmen technische und organisatorische Art ausgewählt werden müssen.

DARF MAN WEITER WERBEN?

Auf Druck der Werbewirtschaft hatte § 28 Abs. 3 BDSG erhebliche Privilegierungen bei der Werbung geregelt. Allein das sogenannte Listenprivileg, wonach bestimmte Arten von sogenannten Listendaten auch ohne Einwilligung der Betroffenen für Werbemaßnahmen genutzt werden konnten, gab erhebliche Gestaltungsmöglichkeiten, die auch bei Verbänden etwa im Bereich der Bewerbung von Fortbildungsaktivitäten oder sonstigen Angeboten des Verbandes kommerzieller Art in der Praxis gerne genutzt wurden. Von daher kann das Bundesdatenschutzgesetz durchaus als werbefreundlich angesehen werden. Solche Privilegien entfallen künftig. Die Datenschutz-Grundverordnung hat keine spezifischen Regelungen für die Werbung unter Ausnutzung personenbezogener Daten, sodass letztlich die Zulässigkeit der Werbung allein nach Art. 6 Abs. 1 lit. f der Grundverordnung im Rahmen einer Interessenabwägung überprüft werden muss, sollte keine Einwilligung vorliegen. Allerdings hilft bei der Auslegung Erwägungsgrund 47 zur Grundverordnung, wonach die Verarbeitung personenbezogener Daten zum Zwecke der Direktwerbung als eine einem berechtigten Interesse dienende Verarbeitung betrachtet werden kann.

Rechtswirksam nach den Bestimmungen des Bundesdatenschutzgesetzes erteilte Einwilligungen zur Werbung sollen fortgelten, sofern sie sich der Art nach den Bedingungen der Datenschutz-Grundverordnung unterwerfen (Erwägungsgrund Nr. 171). Die rein wettbewerbsrechtliche Bestimmung von § 7 UWG gilt fort, sodass schon im bisherigen Recht enthaltene Beschränkungen insbesondere im Zusammenhang mit der Ausnutzung von Mailsystemen für die Werbung weiterhin fortgelten.

Auch das schon bislang im deutschen Recht normierte sogenannte Koppelungsverbot gilt auch nach der Grundverordnung weiter fort. Es soll verhindert werden, dass der Betroffene mit der Zustimmung für eine werbliche Nutzung letztlich mit seinen Daten zahlt, etwa indem er etwa kostenlose Newsletter gegenfinanziert mit der Zustimmung, eigene Daten zur Werbung praktisch freizugeben.

INSGESAMT IST DIE DATENSCHUTZ-GRUNDVERORDNUNG TECHNIKLASTIGER ALS DAS BUNDESDATENSCHUTZGESETZ. SO GREIFT ART. 25 DER GRUND-VERORDNUNG DAS KONZEPT DES DATENSCHUTZES DURCH TECHNIK (PRIVACY BY DESIGN) UND DER NUTZUNG DATENSCHUTZFREUNDLICHER VOREINSTELLUNGEN (PRIVACY BY DEFAULT) AUF.

FAZIT

Es ist sicherlich übertrieben, wenn man behaupten würde, dass ab Mai 2018 alle datenschutzrechtlichen Uhren auf null gestellt werden müssen. Viele Prinzipien, die das deutsche Recht derzeit schon kennt, finden sich auch in der Grundverordnung wieder. Das Problem liegt jedoch woanders: Datenschutz wurde bislang als eine Art lästige Pflicht empfunden, die Geld kostet und nichts bringt. In Ermangelung effektiver Sanktionen und Überprüfungen durch die Behörden konnte man diesen denkbaren „Ansatz“ auch mit guter Aussicht auf Erfolg über einige Jahre fortführen. Diese Zeiten sind jetzt vorbei. Wenn die Behörden personell wie angekündigt stark aufstocken und sich der Bußgeldrahmen verzehnfacht, wird ein datenschutzrechtlicher Blindflug in Zukunft teuer.

Von daher sollten die Verbände rechtzeitig vor Mai 2018 den Status quo im eigenen Haus ermitteln, um dann noch rechtzeitig die Maßnahmen ergreifen zu können, die man unbedingt braucht, um die Konformität des Verbandshandelns mit dem Datenschutz herzustellen. ■

AUTOR

RALF WICKERT

ist Rechtsanwalt und Fachanwalt für Steuer- und Arbeitsrecht. Er ist Gesellschafter der Dornbach GmbH Rechtsanwaltsgesellschaft mit den Tätigkeitsschwerpunkten gesellschaftsrechtlicher, arbeits- und steuerrechtlicher Beratung von Unternehmen und Verbänden.

www.verbaende.com/fachartikel
(geschützter Bereich für Abonnenten und DGVM-Mitglieder)