

Zeit zum Handeln



VON THOMAS ALTHAMMER

Thomas Althammer ist Wirtschaftsinformatiker und verfügt über rund zwanzig Jahre IT-Erfahrung im Gesundheits- und Sozialwesen. Zusammen mit seinen Kollegen begleitet er bundesweit Einrichtungen und Träger als externer Datenschutzbeauftragter und berät zu Fragen der Informationssicherheit und IT-Strategie. Beim Fachverband Informationstechnologie in Sozialwirtschaft und Sozialverwaltung (FINSOZ) e. V. engagiert er sich als Leiter der Arbeitsgruppe IT-Compliance. www.althammer-kill.de

Ab 2018 erhalten alle Mitgliedsstaaten der Europäischen Union neue rechtliche Vorgaben im Datenschutz. Einrichtungen und Träger im Sozialwesen sollten jetzt schon jetzt beginnen, sich mit den Änderungen und Neuerungen auseinanderzusetzen.

Die Europäische Union erhält ein neues Datenschutzrecht: Im letzten Dezember haben Innen- und Rechtsausschuss des EU-Parlaments den lang diskutierten Entwurf der EU-Datenschutzgrundverordnung mit großer Mehrheit angenommen. Zuvor wurde auf informeller Ebene im sogenannten Trilog zwischen Rat, Europäischem Parlament und Europäischer Kommission verhandelt.

Das Verhandlungsergebnis wird derzeit in 22 Sprachen der Mitgliedsländer übersetzt. Parlament und EU-Ministerrat müssen dann über diese übersetzten Fassungen abstimmen. Erst danach erfolgt die Veröffentlichung im Amtsblatt der Europäischen Union.

Damit wird die EU-Datenschutzgrundverordnung offiziell und Unternehmen müssen sich mit den Inhalten auseinandersetzen. Die Verordnung ist zwei Jahre nach Inkrafttreten des Gesetzes, also voraussichtlich ab Sommer 2018, anzuwenden. Auch für Organisationen und Unternehmen stellen sich in diesem Zusammenhang zahlreiche Fragen, die beantwortet sein wollen:

Welchen Einfluss hat die EU-Datenschutzgrundverordnung auf deutsche Gesetze?

Die Datenschutzgrundverordnung der Europäischen Union (EU-DSVGO) muss als Verordnung nicht erst in nationales Recht umgesetzt werden, sondern gilt automatisch in jedem Mitgliedsland. Dadurch werden in Deutschland das Bundesdatenschutzgesetz und die 16

Landesdatenschutzgesetze weitgehend ersetzt.

An ihre Stelle tritt ein Begleitgesetz zur Grundverordnung, das einige Ergänzungen und Besonderheiten regeln wird. Es ist davon auszugehen, dass weitere rechtliche Rahmenbedingungen mit Anknüpfung zum Datenschutz (z. B. Telemediengesetz, Telekommunikationsgesetz, Sozialgesetzbücher) auf notwendige Anpassungen hin überprüft werden.

Was ist als nächstes für Unternehmen zu tun?

Wir empfehlen eine frühzeitige Auseinandersetzung mit der neuen Verordnung und erwarten keine wesentlichen Änderungen mehr in den anstehenden Abstimmungen. Der Übergangszeitraum von zwei Jahren wird erforderlich sein, um die vorhandene Datenschutzorganisation in Unternehmen auf die Bestimmungen der EU-Verordnung umzustellen.

Auch wenn im Kern die Grundfragen des Datenschutzes erhalten bleiben, sind doch Verträge, Formulare und Richtlinien vollständig zu überarbeiten und auf die neue Gesetzesgrundlage anzupassen. Bei der heute häufig unvollständigen Datenschutzorganisation sozialer Einrichtungen handelt es sich dabei um eine teils sehr umfangreiche Aufgabe.

Erste Datenschutz-Aufsichtsbehörden in Deutschland haben begonnen, mit einem Fragebogen die Unternehmen im Hinblick auf die Auseinandersetzung mit der Datenschutzgrundverordnung

der Europäischen Union zu überprüfen. So verschickte der Hessische Datenschutzbeauftragte folgende Fragen:

- Hat Ihr Unternehmen bereits geprüft, ob die von Ihnen durchgeführten Datenverarbeitungsprozesse nach dem aktuellen Stand der Verhandlungen zur Datenschutzgrundverordnung der Europäischen Union zulässig sind?
- Haben Sie bereits einen Plan zur möglicherweise notwendigen Anpassung an die Anforderungen der Datenschutzgrundverordnung der Europäischen Union erstellt?

- Recht auf Vergessen im Internet
- höhere Bußgelder bei Datenschutzverstößen
- Bindung ausländische Unternehmen an das EU-Datenschutzrecht
- Anhebung des Mindestalters für die Einwilligung zur Datenverarbeitung auf 16 Jahre
- Haftung bei Datenschutzverstößen: wichtige Neuerungen bei der Auftragsdatenverarbeitung

Die Einbindung externer Dienstleister wurde auf Basis der bisherigen Gesetze eher stiefmütterlich geregelt. Verträge

cke eine regelmäßige und systematische Beobachtung von betroffenen Personen erforderlich machen.

Aufgenommen wurde in der letzten Phase der Trilog-Verhandlungen eine nationale Öffnungsklausel für die Bestellung eines betrieblichen Datenschutzbeauftragten. Vertreter des Bundesinnenministeriums kündigten an, die Voraussetzungen in einem Verordnungsergänzungsgesetz gegenüber dem Bundesdatenschutzgesetz unverändert zu regeln.

Welche Änderungen sind im kirchlichen Bereich zu erwarten?

Der kirchliche Datenschutz ist von der EU-Datenschutzgrundverordnung zunächst unberührt, wird sich aber – wie schon in der Vergangenheit – an den geltenden Vorschriften orientieren. Insofern ist davon auszugehen, dass das Datenschutzgesetz der evangelischen Kirche (DSG-EKD, gilt u.a. auch für diakonische Einrichtungen) und die Anordnung über den Datenschutz in der katholischen Kirche (KDO, z. B. für Caritas-Einrichtungen relevant) in den kommenden zwei Jahren ebenfalls Anpassungen erfahren werden. ■

»IT-Dienstleister könnten versuchen, Haftungsrisiken auf ihre Auftraggeber abzuwälzen«

Eine Prüfung durch Aufsichtsbehörden scheint zum jetzigen Zeitpunkt etwas verfrüht, denn noch ist die Datenschutzgrundverordnung nicht in Kraft. Die inhaltliche Auseinandersetzung mit den Themen sollte in den Unternehmen aber dennoch bereits beginnen.

Welche Änderungen sind konkret zu erwarten?

Als Verordnung muss die Datenschutzgrundverordnung der Europäischen Union nicht einzeln in nationales Recht umgesetzt werden, sondern gilt nach dem Übergangszeitraum unmittelbar für alle Länder der Europäischen Union. Sie enthält Regelungen unter anderem für folgende Bereiche:

- Vereinheitlichung der Bedingungen zur Verarbeitung personenbezogener Daten durch private und öffentliche Stellen in ganz Europa (weitgehend Ablösung bisheriger Datenschutzgesetze)
- umfangreichere Regelungen bei der Zusammenarbeit mit externen Dienstleistern
- Vereinheitlichung der Auskunftspflichten über gespeicherte Daten, aber auch über Datenverlust und IT-Sicherheitsvorfälle – Stärkung von Verbraucherrechten
- Recht auf Datenportabilität im Internet

zur Datenverarbeitung im Auftrag gehören noch nicht zum Standard, obwohl die Vorgaben über alle Datenschutzgesetze hinweg eindeutig sind.

Mit der Datenschutzgrundverordnung der Europäischen Union haften nun grundsätzlich Auftraggeber und Auftragnehmer gemeinsam gegenüber den Betroffenen (im Sinne eines »joint control«). Damit dürften sich umfangreiche Haftungsrisiken für IT-Dienstleister ergeben, die in Zukunft ein sehr viel größeres Interesse haben werden, ihre Pflichten und Risiken in Verträgen zur Auftragsdatenverarbeitung auf ein Minimum zu reduzieren. Entsprechende Verträge sollten entsprechend sorgfältig verhandelt werden.

Müssen Einrichtungen in Pflege und Sozialwesen auch zukünftig einen Datenschutzbeauftragten bestellen?

Lang diskutiert wurde die Pflicht zur Bestellung von Datenschutzbeauftragten in Unternehmen. Die heutige deutsche Regelung konnte sich nicht EU-weit durchsetzen. Es ist aber beispielsweise eine Bestellpflicht des Datenschutzbeauftragten für öffentliche Stellen und bei Unternehmen vorgesehen, deren Kerntätigkeit aus Verarbeitungsvorgängen besteht, welche auf Grund ihres Wesens, ihres Umfangs oder ihrer Zwe-

Unmittelbar geltendes Recht

Die Datenschutzgrundverordnung ist eine geplante Verordnung der Europäischen Union, mit der die Regeln für die Verarbeitung von personenbezogenen Daten durch private Unternehmen und öffentliche Stellen EU-weit vereinheitlicht werden sollen. Dadurch soll einerseits der Schutz von personenbezogenen Daten innerhalb der Europäischen Union sichergestellt, andererseits der freie Datenverkehr innerhalb des Europäischen Binnenmarktes gewährleistet werden. Die Datenschutzgrundverordnung ist Teil der beabsichtigten EU-Datenschutzreform, welche die Europäische Kommission am 25. Januar 2012 vorgestellt hatte. Mit der Verordnung sollen das Recht auf Vergessenwerden und das Recht auf Datenportabilität eingeführt werden. Sie soll auch für Unternehmen gelten, die ihren Sitz außerhalb der Europäischen Union haben, sich mit ihren Angeboten aber an EU-Bürger wenden.

Quelle: <https://de.wikipedia.org/wiki/Datenschutz-Grundverordnung>