Bank für Sozialwirtschaft

BFS-FACHBEITRAG

01/18

Die Europäische Datenschutzgrundverordnung – Großer Wurf im Datenschutzrecht oder neues Bürokratiemonster?

Stefan Strüwe / David Große Dütting, Curacon GmbH

Ab dem 25. Mai 2018 wird die Europäische Datenschutzgrundverordnung (DS-GVO) für alle Unternehmen verpflichtend anzuwenden sein. Höchste Zeit also, vorhandene Datenschutzmanagementsysteme an die neuen Rahmenbedingungen anzupassen. Dies gilt vor allem für Einrichtungen der Gesundheits- und Sozialbranche, in denen in großem Umfang besondere Kategorien personenbezogener Daten verarbeitet werden. Denn für deren Verarbeitung bestehen hohe gesetzliche Hürden.

Ausgangslage

Im April 2016 wurde nach mehr als vier Jahren Verhandlungszeit die Verordnung 2016/679 oder auch Datenschutzgrundverordnung vom EU-Parlament verabschiedet, welche zum 24. Mai 2016 in Kraft treten konnte. Oberstes Ziel der neuen Verordnung ist die Vereinheitlichung der Regeln für die Verarbeitung und den Schutz von personenbezogenen Daten sowie die Gewährleistung des freien Datenverkehrs im Europäischen Binnenmarkt.
Nach Ablauf der zweijährigen Übergangszeit werden die Anforderungen ab dem 25. Mai 2018 von allen Unternehmen in Europa anzuwenden sein. Besondere Anpassungsbedarfe bestehen dabei in solchen Einrichtungen, die systematisch personenbezogene Daten verarbeiten oder deren Geschäftstätigkeit überwiegend in der Verarbeitung besonderer Kategorien personenbezogener Daten (z. B. Gesundheitsdaten) liegt. Somit dürften im Bereich der Sozialwirtschaft und des Gesundheitswesens nahezu ausnahmslos alle Unter-

nehmen unmittelbar betroffen sein und sind gefordert, die eigenen Geschäftsprozesse zu prüfen und der Verordnung entsprechend anzupassen.

Dritter Weg im Datenschutzrecht bleibt erhalten

Damit die angestrebten Ziele der Verordnung durch die Mitgliedsstaaten nicht unterminiert werden, ist es diesen grundsätzlich nicht erlaubt, die von der Verordnung abgesteckten Anforderungen durch Gesetze abzuschwächen bzw. zu verstärken. Jedoch wird im Rahmen von Öffnungsklauseln die Möglichkeit gegeben, bestimmte Aspekte des Datenschutzes eigenständig zu regeln. Die Bundesrepublik hat diese Möglichkeit im Juni 2017 bereits wahrgenommen und mit dem Datenschutzanpassungs- und Umsetzungsgesetz (DSAnpUG) eine Neufassung des Bundesdatenschutzgesetzes verabschiedet.
Aufgrund des Selbstbestimmungsrechts der Kirchen in Deutschland, eigene Rechtsverordnungen für ihren Geltungsbereich zu bestimmen, galt in Einrichtungen katholischer Trägerschaft bisher die Anordnung über den Kirchlichen Datenschutz (KDO) und in Einrichtungen mit evangelischem Hintergrund das Datenschutzgesetz der Evangelischen Kirche (DSG-EKD). Dem nationalen Gesetzgeber folgend, werden die Kirchen eine Anpassung ihrer Rechtsvorschriften forcieren (müssen), um den höheren Anforderungen der DS-GVO Rechnung zu tragen. Dabei betont die Katholische Kirche durch eine einfache Änderung in der Nomenklatur – aus der Anordnung wird zukünftig das Gesetz über den Kirchlichen Datenschutz (KDG) – die allgemein gesteigerte Bedeutung des Datenschutzes. Sowohl das KDG als auch das DSG-EKD sind im vergangenen November von den jeweiligen Gremien verabschiedet worden und sollen am 24. Mai 2018 in Kraft treten.

Neue und höhere Anforderungen

Schon vor Inkrafttreten der DS-GVO mussten Unternehmen, deren Kerntätigkeit in der Verarbeitung besonderer Kategorien personenbezogener Daten besteht oder in denen mindestens zehn Personen mit der Verarbeitung solcher Daten beschäftigt sind, einen betrieblichen Datenschutzbeauftragten (DSB) bestellen. Durch die Verordnung entfällt nunmehr die Einschränkung auf die Verarbeitung in elektronischen Systemen, sodass auch Personen, die mit der Verwaltung von Akten betraut sind, einzubeziehen sind.
Ähnliches gilt für das Verfahrensverzeichnis, das im Rahmen der DS-GVO als Verzeichnis der Verarbeitungsprozesse bezeichnet wird. Die Notwendigkeit zur Erstellung dieser Übersicht besteht zukünftig ab 250 Beschäftigten oder für kleinere Stellen, wenn die Verarbeitung der Daten die Rechte Betroffener gefährdet, diese nicht nur gelegentlich erfolgt oder besondere Kategorien personenbezogener Daten umfasst. Somit dürften für praktisch alle Einrichtungen der Sozialwirtschaft die Bestellung eines DSB sowie die Erstellung eines Verzeichnisses über die Verarbeitungstätigkeiten verpflichtend werden.
Die Regelungen in der DS-GVO hinsichtlich der Datenverarbeitung im Auftrag entsprechen weitestgehend den bisher geltenden nationalen und kirchenrechtlichen Vorschriften. Neu hinzu kommt die Verpflichtung des Auftraggebers, die Einhaltung der technischen und organisatorischen Maßnahmen beim Auftragnehmer regelmäßig zu überprüfen, alle beim Auftragnehmer mit der Datenverarbeitung betrauten Personen auf die Schweigepflicht zu verpflichten und den Auftragnehmer ebenfalls vertraglich auf die Erstellung des Verzeichnisses über die Verarbeitungstätigkeiten festzulegen. Die neuen Regelungen gelten dabei nicht nur für zukünftige Vertragsabschlüsse, sondern auch für alle vorhandenen und laufenden Verträge, was die Überprüfung und Anpassung dieser notwendig macht.

Gestärkte Betroffenenrechte

Höhere Anforderungen ergeben sich des Weiteren bezüglich der Informationspflichten gegenüber Betroffenen und der Umsetzung ihrer Rechte, welche durch die DS-GVO eine deutliche Stärkung erfahren. So können Betroffene im Vorfeld, während und nach der Verarbeitung, zahlreiche Rechte wahrnehmen, die sich entlang des Prozesses der Datenverarbeitung ziehen: So sind die Betroffenen vor der Verarbeitung präzise und verständlich über die Verarbeitung ihrer personenbezogenen Daten aufzuklären. Diese Information hat in einer einfachen und klaren Sprache zu erfolgen. Daneben setzen das Auskunftsrecht sowie das Recht auf Berichtigung den Fokus auf den aktiven Verarbeitungsprozess. Die Rechte zur Datenlöschung, auf Einschränkung der Verarbeitung sowie auf Datenübertragbarkeit werden hingegen am Ende des Prozesses wahrgenommen. Bei Letzterem handelt es sich um ein durch die DS-GVO neu geschaffenes Recht, das dem Betroffenen die Möglichkeit eröffnet, gespeicherte Daten (z. B. in Sozialen Medien) an andere Anbieter zu übertragen. Unternehmen sind gefordert, bis zum 25. Mai 2018 die prozessualen und technischen Voraussetzungen zur Wahrnehmung der Betroffenenrechte zu schaffen.

Technischer Datenschutz

Mit Art. 25 enthält die DS-GVO darüber hinaus eine Neuerung, die die Einhaltung der Datenschutzgrundsätze durch die aktive Gestaltung von Technik („Privacy by Design“) und der datenschutzfreundlichen Voreinstellung („Privacy by Default“) zu forcieren versucht. Einrichtungen der Sozialwirtschaft werden, vor allem vor dem Hintergrund der zunehmenden Digitalisierung ihrer Geschäftsprozesse, diese Aspekte bereits bei der Planung und Entwicklung neuer Produkte und Dienstleistungen berücksichtigen müssen.
Die DS-GVO gibt außerdem vor, dass der technische Datenschutz unter Berücksichtigung des Stands der Technik umzusetzen ist. Die aktuelle Situation kann daher als allgegenwärtige und akzeptierte Rechtsverletzung aufgefasst werden, mit der Folge, dass bisher nur massive Übertretungen geahndet wurden. Dies sollte Unternehmen jedoch nicht dazu verleiten, eine abwartende Haltung zu beziehen, denn einige Juristen sehen die Umsetzung von „Privacy by Design“ bereits jetzt als Verpflichtung an. So urteilte das Bundessozialgericht in einem Fall aus 2012 (Az.: B 1 KR 13/12 R) gegen eine Krankenkasse, die einem Auskunftsgesuch einer Betroffenen nicht nachkommen wollte, mit der Begründung, dass der Aufwand einer Datensuche im eigenen System zu hoch sei. Das Gericht ließ dies nicht gelten und verwies darauf, dass eine entsprechende Funktion bereits bei der Entwicklung des Systems hätte Berücksichtigung finden müssen.

Ebenfalls neu: Die Folgenabschätzung

Gänzlich neu ist die Pflicht zur Vornahme einer Datenschutz-Folgenabschätzung (DSFA), wenn die Form der Verarbeitung, insbesondere beim Einsatz neuer Technologien, voraussichtlich ein hohes Risiko für die Rechte natürlicher Personen zur Folge hat. Die DSFA muss neben der systematischen Beschreibung der geplanten Verarbeitungsvorgänge auch eine Bewertung der Notwendigkeit und Verhältnismäßigkeit hinsichtlich des Zwecks der Verarbeitung vornehmen sowie die Risiken anhand von Eintrittswahrscheinlichkeit und Schwere bewerten. Schließlich sind geplante Abhilfemaßnahmen zur Bewältigung der identifizierten Risiken darzustellen. Die Abschätzung erweitert damit die bisher durchzuführende Vorabkontrolle, bedingt im Vergleich zu dieser jedoch einen deutlich gestiegenen Aufwand.

Dies bestätigte jüngst das Bayrische Landesamt für Datenschutzaufsicht, dass die DSFA als „nicht trivialen“ Prozess bezeichnete, da diese eine systematische Vorgehensweise in Verbindung mit sehr ausführlichen Dokumentationsanforderungen erfordere. Dabei bestehen allgemein noch große Unsicherheiten, wie genau die Abschätzung durchzuführen ist. Zwar liegen bereits Versuche der Aufsichtsbehörden vor, diese prozessmäßig zu beschreiben, jedoch dürften die Vorschläge nur durch Großunternehmen umsetzbar sein. So fehlt es noch an einer übersichtlichen und schnell abzuarbeitenden Beschreibung, mit welcher kleinen und mittelgroßen Unternehmen die Möglichkeit gegeben wird, mit angemessenen Mitteln ihrer Pflicht nachzukommen. Daher sollten Unternehmen neue Veröffentlichungen der Aufsichtsbehörden im Auge behalten, um möglichst frühzeitig darauf reagieren zu können.

Enges Zeitfenster, drakonische Strafen

Die zuvor genannten Punkte sind nur eine Auswahl der neuen Anforderungen aus der DS-GVO, machen jedoch deutlich, wie umfangreich die Anpassungsbedarfe für die Unternehmen sind. Aktuell verbleiben nicht einmal mehr vier Monate, bis die neuen gesetzlichen Grundlagen Anwendung finden. Erfahrungen haben gezeigt, dass allein die Erstellung eines Verzeichnisses der Verarbeitungstätigkeiten oftmals weit mehr Zeit in Anspruch nimmt.
Bisher waren hohe Bußgelder in Deutschland die Ausnahme und bewegten sich zumeist im fünfstelligen Bereich. Die höchsten bekannten Zahlungen mussten eine Versicherung wegen gesetzeswidrige Erwerbs von Listen mit potenziellen Kunden in Höhe von 1,3 Mio. Euro sowie die Deutsche Bahn wegen illegaler Massen-Screenings ihrer Mitarbeiter mit insgesamt 1,1 Mio. Euro zahlen. Zukünftig werden Verstöße gegen das geltende Datenschutzrecht wahrscheinlich häufiger solche Dimensionen erreichen. So schreibt die DS-GVO die Verhängung von Geldbußen in Höhe von 2 % des gesamten, konzernweiten Jahresumsatzes oder max. 10 Mio. Euro bzw. von 4 % oder max. 20 Mio. Euro bei besonders schweren oder wiederholten Verstößen vor. Unternehmen sollten daher die gesetzlichen Anforderungen bis Mai 2018 umsetzen und im Falle einer Auseinandersetzung einen kooperativen Umgang mit den Aufsichtsbehörden pflegen bzw. frühzeitig in Kommunikation mit diesen treten.

Umsetzung der Grundverordnung

Die Umsetzung der vielfältigen Anforderungen aus der DS-GVO setzt voraus, dass hierfür ausreichend Ressourcen zur Verfügung gestellt und die organisatorischen Rahmenbedingungen definiert werden. Hierzu sollten zunächst auf Ebene der Geschäftsführung die Zuständigkeiten geregelt sowie die Organisationsstandards festgelegt werden, die zum einen den neuen gesetzlichen Anforderungen entsprechen und zum anderen die individuellen Gegebenheiten des Unternehmens abbilden. Hieraus lässt sich eine Datenschutzstrategie ableiten, die von der Geschäftsführung in Kraft gesetzt und den Mitarbeitern als verbindliche Vorgabe kommuniziert wird.
Daran anschließend sollte die Prozesslandschaft risikoorientiert dahingehend analysiert werden, ob die vorhandenen Prozesse mit den Vorgaben aus Gesetzen, Standards und Strategie kongruent sind und unter Umständen einer Neujustierung bedürfen. Der Fokus sollte hierbei auf der Rechenschaftspflicht liegen, damit die entsprechenden Dokumente aus dem jeweiligen Workflow generiert und – im Falle der Prüfung – den Aufsichtsbehörden vorgelegt werden können. Für alle Datenverarbeitungen sind dem jeweiligen Schutzbe-

darf entsprechende technische und organisatorische Maßnahmen zu treffen; deren Entwicklungsprozess ist zu dokumentieren. Die Maßnahmen sind sodann umzusetzen und regelmäßig, z. B. in Form von Audits, auf ihre Wirksamkeit und Aktualität zu prüfen.
Um der Forderung nach kontinuierlicher Weiterentwicklung nachzukommen, empfiehlt sich des Weiteren eine Orientierung am etablierten Demingkreis. So können mit der systematischen Durchführung risikoorientierter Audits (PLAN) die bestehenden Geschäftsprozesse auf die Datenschutzkonformität überprüft werden (CHECK) und auf Grundlage dieser Ergebnisse Gegenmaßnahmen bzw. Anpassungen erarbeitet und implementiert werden (ACT). Abschließend sind im Rahmen eines zu installierenden Kontrollsystems zielführende Datenschutzkontrollen in den Workflow zu integrieren, deren Durchführung ebenfalls des dokumentierten Nachweises bedarf. Die Überwachung der Kontrollen kann an den Datenschutzbeauftragten delegiert werden, welcher für die Mitarbeiter ebenfalls erster Ansprechpartner ist (DO). Vor diesem Hintergrund ist empfehlenswert, dass das Datenschutzmanagement an bereits bestehende Qualitätsmanagementsysteme angeknüpft wird, um so vorhandenes Wissen effizienter zu nutzen und Verbundeffekte heben zu können.

Fazit

Es bleibt festzuhalten, dass die DS-GVO vor allem wegen der gesteigerten Bedeutung der Rechenschaftspflicht für die meisten Unternehmen zu einem deutlichen Mehraufwand im Bereich des Datenschutzmanagements führen wird. Diesen werden die Unternehmen aufgrund der hohen Strafen bei Verstößen gegen die gesetzlichen Anforderungen aber in Kauf nehmen müssen. Nutzen Unternehmen dabei jedoch bereits vorhandene Ressourcen aus dem Risiko- und Qualitätsmanagement, lässt sich dieser Mehraufwand leichter verkraften.
Allen Unkenrufen zum Trotz ist auch anzuerkennen, dass die DS-GVO für die Betroffenen die Möglichkeiten zur Durchsetzung ihrer Rechte deutlich vereinfacht und insbesondere vor dem Hintergrund der zunehmenden Datensammelwut großer Konzerne sowie dem Megatrend der Digitalisierung ein zeitgemäßes Regelwerk darstellt.

Autoren:

Stefan Strüwe, Rechtsanwalt und Seniormanager im Geschäftsfeld Datenschutz, Curacon GmbH, E-Mail: stefan.struewe@curacon.de / David Große Dütting, Berater und Fachkraft für Datenschutz, Curacon GmbH, E-Mail: david.grosse-duetting@curacon.de

Dieser Beitrag wurde veröffentlicht in der BFS-Info 1/18.

Impressum

Bank für Sozialwirtschaft
Aktiengesellschaft
Wörthstraße 15 – 17
50668 Köln

Registereintrag für den Sitz Köln
Handelsregister des Amtsgerichts Köln
Registernummer HRB 29259

Registereintrag für den Sitz Berlin
Handelsregister des Amtsgerichts Berlin-Charlottenburg
Registernummer: HRB 64059
Umsatzsteuer-ID: DE 136634199

Vorstand
Prof. Dr. Harald Schmitz (Vorsitzender)
Thomas Kahleis | Oliver Luckner

Aufsichtsratsvorsitzender
Dr. Matthias Berger

Kontakt
Telefon 0221 97356-0
Telefax 0221 97356-219
E-Mail bfs@sozialbank.de

Aufsichtsbehörde
Bundesanstalt für
Finanzdienstleistungsaufsicht (BaFin)
Sitz Bonn
Graurheindorfer Straße 108
53117 Bonn

Wir sind Mitglied im Bundesverband der Deutschen Volksbanken und Raiffeisenbanken - BVR und der Sicherungseinrichtung angeschlossen.