Betriebswirtschaftliche Blätter

14. Februar 2018 - 08:30 | EU-DSGVO

Datenschutz im Fokus der Auftragsverarbeitung

Daniel Nyhof, Dr. Gregor Vogt

Der Countdown, die neuen gesetzlichen Anforderungen an Datenschutz und -sicherheit zu erfüllen, läuft: Ab dem 25. Mai muss jedes Unternehmen die Vorgaben der Europäischen Datenschutzgrundverordnung (EU-DSGVO) und des neuen Bundesdatenschutzgesetzes (BDSG neu) erfüllen.

Eine Kurzzusammenfassung finden Sie hier.

Ab 25. Mai muss jedes Unternehmen die Vorgaben der EU-DSGVO erfüllen. (Oakozhan/fotolia)

Ziel von EU-DSGVO und BDSG neu ist eine angemessene Balance zwischen Wirtschafts- und Verbraucherinteressen im Zeitalter der Digitalisierung, um damit innerhalb Europas ein einheitliches Datenschutzniveau zu schaffen. Wer die Vorgaben nicht einhält oder gar missachtet, kann mit drastischen Geldbußen bis zu 20 Millionen Euro oder maximal vier Prozent des Jahresumsatzes bestraft werden.
Im Vergleich zu den europäischen Nachbarländern gibt es in Deutschland durch das bisherige BDSG bereits hohe Anforderungen an den Datenschutz. Unternehmen, die in der Vergangenheit alle notwendigen organisatorischen und technischen Maßnahmen zur Erfüllung der gesetzlichen Vorgaben umgesetzt haben, verfügen über eine gute Ausgangsbasis. Die EU-DSGVO regelt das gesamte Datenschutzrecht neu und gilt unmittelbar als anwendbares Recht in jedem Mitgliedstaat (Anwendungsvorrang). Es baut an vielen Stellen auf bisherigen Standards und Erfahrungen auf, wird aber deutlich umfangreicher und komplexer.

Öffnungsklauseln bieten Spielraum für den nationalen Gesetzgeber. Zum Teil ist auch eine Ausgestaltungspflicht für die Mitgliedstaaten angeordnet. Im Rahmen des "Datenschutz-Anpassungs- und Umsetzungsgesetzes" (DSAnpUG-EU) wird das neue BDSG mit der EU-DSGVO am 25. Mai wirksam und umfasst nahezu doppelt so viele Paragrafen wie das bisherige BDSG. Schon jetzt zeichnet sich ab, dass der Dokumentations- und Bearbeitungsaufwand deutlich zunehmen

wird. Mit der EU-DSGVO wird die künftige "Auftragsverarbeitung" erstmals europaweit einheitlich geregelt. Die deutschen Vorschriften dazu sind zu einem großen Teil in die neuen europäischen Vorschriften eingeflossen.

Neue Begriffe und Definitionen

Art. 4 enthält zahlreiche Begriffsbestimmungen, die teilweise bereits im BDSG verwendet und in der EU-DSGVO jedoch neu ausgelegt, erweitert oder klargestellt worden sind: Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen, vor allem auch Onlinekennungen mittels IP-Adresse oder Cookies, die eine eindeutige Zuordnung ermöglichen. Der neue Verarbeitungsbegriff umfasst jetzt alle Verarbeitungsphasen, eine Differenzierung zwischen Erhebung, Verarbeitung oder Nutzung erfolgt nicht mehr.

Bedingt durch den neuen Rechtsrahmen ist künftig die europäische Auslegung bzw. Rechtsprechung maßgeblich. Um zur einheitlichen Anwendung der neuen Verordnung in der gesamten Union beizutragen, sieht Art. 63 EU-DSGVO ein Kohärenzverfahren der nationalen Aufsichtsbehörden vor, die aufgefordert sind, untereinander und gegebenenfalls mit der EU-Kommission zusammenzuarbeiten. Bis zur Klärung der diversen Auslegungsfragen bleibt somit für eine bestimmte Zeit eine Rechtsunsicherheit bestehen.

Grundsätze und Rechtmäßigkeit

Die Grundsätze für die Verarbeitung gemäß Art. 5 EU-DSGVO sind größtenteils bekannt: Grundsatz der Rechtmäßigkeit, der Verarbeitung nach Treu und Glauben, der Zweckbindung, der Datensparsamkeit, der Richtigkeit und der Begrenzung der Speicherdauer sowie Integrität und Vertraulichkeit. Vor allem der Grundsatz der Rechtmäßigkeit wird in Art. 5 Abs. 1 lit. b) EU-DSGVO durch eine enge Auslegung der "Zweckbindung" nochmals gestärkt. Der Verantwortliche ist für die Einhaltung verantwortlich und muss Nachweise erbringen können (Rechenschaftspflicht).

In Art. 6 EU-DSGVO sind die verschiedenen Rechtsgrundlagen festgehalten, von denen mindestens eine gegeben sein muss, damit die Verarbeitung rechtmäßig ist. Somit gilt weiterhin das Verbot mit Erlaubnisvorbehalt: Einwilligung, Erfüllung eines Vertrags oder vorvertraglicher Maßnahmen, Erfüllung einer rechtlichen Verpflichtung, Schutz lebenswichtiger Interessen etc.

Vorrangiges Ziel ist der Schutz der Persönlichkeitsrechte. Deshalb sieht die EU-DSGVO eine deutliche Ausweitung der Informationspflichten und eine Stärkung der Rechte der betroffenen Person vor. In diesem Zusammenhang fordert Art. 12 EU-DSGVO präzise, transparente und verständliche Informationen und Mitteilungen gegenüber betroffenen Personen, die sich auf die Verarbeitung ihrer Daten beziehen. Sie sind in einer klaren und einfachen Sprache zu übermitteln.

Die Informationspflichten sind künftig an strenge Formvorschriften gebunden und werden in Art. 13 und 14 konkretisiert. Zum Zeitpunkt der Erhebung der Daten hat der Verantwortliche die betroffene Person umfassend über Zweck sowie Rechtsgrundlage für die Verarbeitung (gegebenenfalls das berechtigte Interesse gemäß Art. 6 Abs 1. lit. f), Empfänger der Daten etc. zu informieren. Um eine faire und transparente Verarbeitung zu gewährleisten, ist die betroffene Person darüber hinaus über die Dauer der Speicherung (gegebenenfalls über Kriterien für die Festlegung der Dauer), seine Auskunftsrechte, Recht auf Berichtigung und Löschung, Einschränkung der Verarbeitung, Widerspruchsrecht, Recht auf Datenübertragbarkeit (Datenportabilität) sowie auf das Recht der Löschung im Sinne des

"Vergessenwerdens" (z. B. bei Widerruf der Einwilligung) hinzuweisen. Zudem muss die betroffene Person auf das Beschwerderecht bei der ständigen Aufsichtsbehörde informiert werden.

Die vorgenannten Auskünfte sind gemäß Art. 14 EU-DSGVO in ähnlicher Weise vom Verantwortlichen zu erteilen, sofern die Daten nicht bei der betroffenen Person erhoben worden sind. Auch die Kontaktdaten des Datenschutzbeauftragten müssen mitgeteilt werden. Diese Ausgangssituation trifft in der Regel bei Beauftragung eines Inkassodienstleisters zu. Die personenbezogenen Daten des Schuldners sind zuvor beim Gläubiger erhoben und mit Erteilung des Inkassoauftrags an den Dienstleister weitergegeben worden. Spätestens zum Zeitpunkt der ersten Korrespondenz zwischen Inkassounternehmen und Schuldner müssen die Informationen gemäß Art. 14 erteilt und über das berechtigte Interesse gemäß Art. 6 Abs. 1f informiert werden.

Auftragsdatenverarbeitung nach BDSG

(BBL)

Der Umgang mit sensiblen, personenbezogenen Daten ist für die Bad Homburger Inkasso (BHI) als Dienstleister und Outsourcing-Partner der Sparkassen-Finanzgruppe von jeher ein wesentlicher Erfolgsfaktor.
Beim Outsourcing des Forderungsmanagements handelt es sich im Sinne des Kreditwesengesetzes (KWG) nach § 25a Abs. 2 um eine Auftragsdatenverarbeitung, die dem Auftraggeber als "Herr des Verfahrens" umfassende Kontroll- und Prüfungsbefugnisse sowie allgemeine Weisungsrechte einräumt. Nach bisheriger Rechtslage wird die BHI im Rahmen der Auftragsdatenverarbeitung gemäß § 11 Bundesdatenschutzgesetz (BDSG) tätig *(s. Abb. 1).* Zuletzt hatte der Gesetzgeber im Jahr 2009 die Regelungen zur Auftragsdatenverarbeitung angepasst. Auftraggeber sind unter anderem gesetzlich dazu verpflichtet worden, sich vor Beginn der Datenverarbeitung und sodann regelmäßig beim Auftragnehmer von der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen (sogenannte TOMs) zu überzeugen. Umsetzung und Erfüllung dieser gesetzlichen Anforderungen sind seither fester Bestandteil der Inkasso-Rahmenverträge und entsprechen den Outsourcingstandards des Deutschen Sparkassen- und Giroverbands (DSGV).

Auftragsverarbeitung nach EU-DSGVO

Die Regelungen zur Auftragsverarbeitung, vor allem die Anforderungen an den Verantwortlichen und den Auftragsverarbeiter, finden sich in Art. 28 EU-DSGVO - inhaltlich stark angelehnt an § 11 BDSG. In der Tiefe gehen die neuen Regelungen jedoch über das heutige Niveau hinaus, indem neue Anforderungen an die Auftragsverarbeitung gestellt werden. So hat der Auftragsverarbeiter hinreichende Garantien für die Einhaltung des Datenschutzes zu gewährleisten, die entsprechend nachzuweisen sind. Diese Nachweise und Garantien können durch entsprechende Zertifizierungen erbracht werden.

Auch nach künftigem Datenschutzrecht steht begrifflich die "Beauftragung eines anderen" im Fokus der Auftragsverarbeitung, sodass weiterhin ein entsprechendes Unterordnungsverhältnis besteht. Im Namen des Verantwortlichen übernimmt der Auftragsverarbeiter die Verarbeitung und darf die Daten gemäß Art. 29 EU-DSGVO ausschließlich auf Weisung des Verantwortlichen verarbeiten.

Nach der neuen Definition des Verantwortlichen tritt der Gedanke, dass dieser Verantwortlicher für das Verfahren ist, noch deutlicher hervor als nach bisherigem nationalem Recht. Der Verantwortliche entscheidet über Zweck und

Mittel der Verarbeitung personenbezogener Daten. Die Beauftragung des Inkassodienstleisters stellt die Entscheidung über das Mittel der Verarbeitung dar, in dem Fall nicht selbst das Inkasso der Forderung zu besorgen, sondern damit einen spezialisierten Dienstleister zu beauftragen. Auch der Zweck wird durch Weisungen von der Sparkasse als Verantwortlichem bestimmt, und nur diese behält sich umfassende Rechte zur Steuerung vor.

Spiegelbildlich dazu steht das Inkassounternehmen als Auftragsverarbeiter nach Art. 4 Nr. 8 EU-DSGVO. Der Dienstleister übernimmt die Inkassobearbeitung im Auftrag und nach Weisung des Verantwortlichen und erfüllt lediglich die vom Auftraggeber festgelegten Vorgaben im Rahmen der getroffenen vertraglichen Vereinbarungen und vor dem Hintergrund des jeweiligen Auftragsverhältnisses. Die BHI als Dienstleister der Sparkassen handelt somit nur weisungsabhängig für den Auftraggeber und kann nicht frei und abschließend über die Datenverarbeitung entscheiden.

Der Inkassodienstleister ist vertraglich gebunden, behält sich keine Rechte auf Zweckänderung vor und unterwirft sich entsprechend dem Auftrag und der Verantwortung des Auftraggebers. Infolgedessen bleibt auch die bereits aus dem BDSG bekannte Rechtsfolge erhalten: Nach Art. 4 Nr. 10 EU-DSGVO ist ein Auftragsverarbeiter nicht Dritter im Sinne des Datenschutzrechts und es findet keine Übermittlung statt. Die BHI als Auftragsverarbeiter der Sparkassen ist folglich nicht als Dritter anzusehen.

Aufsichtsrechtliche Vorgaben

Aufgrund zahlreicher Verpflichtungen von Sparkassen aus dem Bankaufsichtsrecht, allen voran §§ 25a, 25b KWG und den MaRisk, wie auch den entsprechenden Regelungen der Sparkassen-Finanzgruppe, etwa aus der OPDV-Stellungnahme 1/2009, ist das Interesse groß, auch künftige Auslagerungen revisionssicher und aufsichtsgerecht auszugestalten. Der Gesetzgeber hat in den vergangenen Jahren umfangreiche Neufassungen der Regelungen zur Geschäftsorganisation und zum Risikomanagement nach § 25a KWG sowie Auslagerungen und Dienstleistersteuerung nach § 25b KWG vorgenommen.

Die Pflichten für eine ordnungsgemäße Geschäftsorganisation sind dabei entsprechend konkretisiert und vielfach noch umfangreicher definiert. Auch nach dem neuen § 25a KWG sind die allgemeinen Anforderungen an die Ordnungsmäßigkeit bei "nicht wesentlichen Auslagerungen" zu erfüllen. Die gesetzlichen Vorgaben im Aufsichtsrecht werden durch die Erläuterungen der MaRisk ergänzt. Bereits in den vorangegangenen MaRisk-Novellen hat sich eine stärkere Betonung der Überwachung des Outsourcings gezeigt. Die vielfältigen Anforderungen aus KWG und MaRisk zu erfüllen, kann daher weiterhin nur im Rahmen einer Auftragsverarbeitung wirksam umgesetzt werden - vor allem in Fragen der notwendigen und umfangreichen Weisungs- und Kontrollrechte, die vorbehalten sein müssen.

Neue Regelung zur Haftung

Grundsätzlich hat jede Person nach Art. 82 EU-DSGVO, der wegen eines Verstoßes gegen die Verordnung ein materieller oder immaterieller Schaden entstanden ist, Anspruch auf Schadenersatz gegen den Verantwortlichen oder den Auftragsverarbeiter. Nach BDSG haftete bisher ausschließlich die verantwortliche Stelle gegenüber dem Betroffenen. Künftig haftet der Auftragsverarbeiter für einen verursachten Schaden, wenn er seinen speziell auferlegten Pflichten aus der Verordnung nicht nachgekommen ist oder erteilte Weisungen des Verantwortlichen nicht beachtet hat. Sanktionen der Aufsichtsbehörden können auch gegenüber dem Auftragsverarbeiter verhängt werden und sind damit deutlich verschärft worden. Sie sollen in jedem Einzelfall wirksam, verhältnismäßig und abschreckend sein.

Sind sowohl ein Verantwortlicher als auch ein Auftragsverarbeiter an derselben Verarbeitung beteiligt, so haftet gemäß Art. 82 Abs. 4 EU-DSGVO jeder Verantwortliche und Auftragsverarbeiter für den gesamten Schaden (gesamtschuldnerische Haftung), damit ein wirksamer Schadenersatz für die betroffene Person sichergestellt ist.

Meldepflichten bei Verletzungen

Bei Verstößen oder gar Missachtung der Datenschutzvorgaben drohen drastische Geldbußen. *(3dkombinat/ fotolia)*

Bisher hat sich die Informationspflicht nach § 42a BDSG bei unrechtmäßiger Kenntniserlangung auf bestimmte Datenkategorien wie besondere Arten personenbezogener Daten und Daten zu Bank- oder Kreditkartenkonten etc. beschränkt. Diese Eingrenzung fällt gänzlich weg. Bei der "Verletzung des Schutzes personenbezogener Daten" handelt es sich nach Art. 4 Abs. 12 EU-DSGVO um eine Verletzung der Sicherheit, die zur Vernichtung, zum Verlust oder zur Veränderung personenbezogener Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet worden sind.

Der Verantwortliche hat unverzüglich und möglichst binnen 72 Stunden, nachdem die Verletzung bekannt geworden ist, eine Meldung an die zuständige Aufsichtsbehörde vorzunehmen (Art. 33 Abs. 1 EU-DSGVO) - es sei denn, die Verletzung führt voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen.

Wenn eine Verletzung des Schutzes personenbezogener Daten dem Auftragsverarbeiter bekannt wird, hat er diese unverzüglich dem Verantwortlichen zu melden (Art. 33 Abs. 2 EU-DSGVO). Auch die betroffene Person ist unverzüglich von der Verletzung zu benachrichtigen, sofern ein hohes Risiko für die persönlichen Rechte und Freiheiten als Folge nicht ausgeschlossen werden kann (Art. 34 EU-DSGVO).

Umsetzung der EU-DSGVO bei der BHI

In den vergangenen Monaten hat die BHI unter Einbindung des Datenschutzbeauftragten sämtliche organisatorischen und technischen Arbeitsabläufe auf die Anforderungen der EU-DSGVO hin durchleuchtet. Die operative Umsetzung erfolgt im Rahmen eines Projekts, das bis Mitte April 2018 abgeschlossen sein wird. Zu den Maßnahmen gehören unter anderem:

- Überprüfung und Anpassung von Prozessen hinsichtlich der Rechte betroffener Personen und Kommunikation mit der Aufsichtsbehörde,
- neu aufgesetzter Meldeprozess bei Datenpannen vor allem zur Gewährleistung einer schnellen Reaktion,
- Implementierung einer Datenschutz-Folgeabschätzung bei riskanten Verarbeitungen,
- Anpassung der Dokumentationen zur Gewährleistung der Nachweisbarkeit,
- Berücksichtigung der neuen Anforderungen in der Schuldnerkorrespondenz zur Erfüllung der Informationspflichten,
- Überprüfung des Schufa-Meldeverfahrens,

- Fortentwicklung des Verfahrensverzeichnisses zum Verzeichnis von Verarbeitungstätigkeiten,
- Erstellung eines Verzeichnisses von Verarbeitungstätigkeiten der BHI für Auftragsverarbeitungen,
- Überarbeitung der Mandantenverträge für die Auftragsverarbeitung (z. B. Aufnahme des neuen Katalogs mit Pflichtinhalten, Bewertung der Haftungsrisiken und Umsetzung in den Verträgen, Anpassung der Regelungen für die Beauftragung von Subunternehmen),
- Schulungskonzept für Mitarbeiter,
- Zertifizierung der BHI gemäß EU-DSGVO nach Zulassung neuer vom Gesetzgeber zugelassener Zertifizierungsverfahren.

Fazit

Im Zeitalter der Digitalisierung sind Daten ein kostbares Wirtschaftsgut. Ein professionelles Datenmanagement schafft Sicherheit für alle Beteiligten und reduziert Risiken, die es gänzlich zu vermeiden gilt. Die auf Basis der Auftragsverarbeitung ausgestalteten Mandantenverträge der BHI bieten ein Höchstmaß an Sicherheit im Hinblick auf Transparenz, Umsetzung und Kontrolle der gesetzlichen Anforderungen.

Autoren
Daniel Nyhof ist Mitarbeiter der S-Consit GmbH und als Datenschutzbeauftragter für die Bad Homburger Inkasso GmbH tätig.
Dr. Gregor Vogt ist Leiter Entwicklung und Organisation der Bad Homburger Inkasso GmbH.