Lizenziert für Frau Daniela Gaub.
Die Inhalte sind urheberrechtlich geschützt.

04.17

PinG

Privacy in Germany

Datenschutz und Compliance

5. Jahrgang
Juli 2017
Seiten 129–164

www.PinGdigital.de

Redaktion:

Prof. Niko Härting
Dr. Niclas Krohm
Dr. Carlo Piltz
Sebastian Schulz

Ständige Mitarbeiter:

Dr. Sebastian J. Golla
Dr. Jana Moser
Philipp Müller-Peltzer
Frederick A. Richter, LL.M.
Prof. Dr. Jan Dirk Roggenkamp
Daniel Schätzle
Dr. Rainer Stentzel
Jan-Christoph Thode

PRIVACY TOPICS

O. Tene/G. Zanfir-Fortuna
Chasing the Golden Goose: What is the path to effective anonymisation?

J. Eichenhofer
Vom Zweckbindungsgrundsatz zur Interessenabwägung

PRIVACY NEWS

M.W. Mosing
Österreich: Entwurf des Datenschutz-Anpassungsgesetzes 2018 – zwischen Evolution durch die Union und Tradition!

S. Rosenthal/F. Trautwein
NIS-Richtlinie und IT-Sicherheitsgesetz in 2017

PRIVACY COMPLIANCE

C. Volkmer/I. Kaiser
Das Verzeichnis von Verarbeitungstätigkeiten und die Datenschutz-Folgenabschätzung in der Praxis

D. Gaub/K.U. Berg
Leitfäden zur Anwendung und Umsetzung der DSGVO – Hinweise zur Erstellung am Beispiel des Best Practice Guides 1.0 für den Bereich des Forderungsmanagements

K.-U. Plath
„The MLAT-Route“

ESV ERICH SCHMIDT VERLAG

86118

© Copyright Erich Schmidt Verlag GmbH & Co. KG, Berlin 2017 - (http://www.pingdigital.de) 11.07.2017 - 08:27
587013053879

Lizenziert für Frau Daniela Gaub.
Die Inhalte sind urheberrechtlich geschützt.

Daniela Gaub ist Referentin für Rechtspolitik beim Bundesverband Deutscher Inkasso-Unternehmen e.V. (BDIU).

Leitfäden zur Anwendung und Umsetzung der DSGVO – Hinweise zur Erstellung am Beispiel des Best Practice Guides 1.0 für den Bereich des Forderungsmanagements

Rechtsanwalt Kay Uwe Berg ist Hauptgeschäftsführer des Bundesverbandes Deutscher Inkasso-Unternehmen e.V. (BDIU).

Daniela Gaub und *Kay Uwe Berg*

Der Bundesverband Deutscher Inkasso-Unternehmen e.V. (BDIU) hat als einer der Ersten einen Best Practice Guide[1] erstellt, mit dem nicht nur ein Überblick zu den einzelnen Regelungen der Europäischen Datenschutz-Grundverordnung gegeben wird, sondern mit dem auch erste Beispiele, Tipps und Hinweise aufgezeigt werden, wie die rechtlichen Anforderungen in der Praxis umgesetzt werden können. Mit dem folgenden Beitrag werden der Hintergrund, der Unterschied zu Verhaltensregeln nach Art. 40 DSGVO, ein Kurzüberblick zum Inhalt sowie die Entwicklung des Leitfadens dargestellt.

I. Hintergrund

Spätestens seitdem die Europäische Datenschutz-Grundverordnung (DSGVO) am 25. Mai 2016 in Kraft getreten und damit klar ist, dass sie genau zwei Jahre später Anwendung finden wird, heißt es Ärmel hochkrempeln, um die nach der DSGVO für die Datenverarbeitungen Verantwortlichen auf das neue Datenschutzrecht ab dem 25. Mai 2018 vorzubereiten.

Für den Bundesverband Deutscher Inkasso-Unternehmen e.V. (BDIU) stand schnell fest, dass die Mitgliedsunternehmen, aber auch darüber hinaus Interessierte und im Forderungsmanagement Tätige bei der Umstellung auf die neuen Anforderungen unterstützt werden müssen. Viele der insgesamt 560 BDIU-Mitgliedsunternehmen sind Einzel- und kleine Unternehmen, die oftmals keinen Datenschutzbeauftragten haben und bei datenschutzrechtlichen Fragen auf externen Input angewiesen sind. Damit sich nicht jedes Unternehmen für sich überlegen muss, wie die DSGVO-Vorgaben in der Praxis berücksichtigt werden müssen, wollte der Verband für alle erste Hinweise geben, wie Datenflüsse und Datenverarbeitungen künftig vonstatten gehen werden.

II. Verhaltensregeln gemäß Art. 40 DSGVO versus Best Practice Guide

1. Überblick

Eine Möglichkeit dazu wäre gewesen, dass sich der BDIU an die Ausarbeitung von Verhaltensregeln im Sinne von Art. 40 DSGVO macht. Art. 40 Abs. 2 DSGVO regelt nämlich, dass Verbände und andere Vereinigungen, die Kategorien von Verantwortlichen und Auftragsverarbeitern vertreten, solch grundlegende Handlungsorientierungen entwickeln können, um die wirksame Anwendung der Verordnung zu erleichtern und die Verordnungsvorgaben zu präzisieren. Solche Regeln können sowohl von nationalen als auch europäischen Verbänden entwickelt werden; die DSGVO stellt dazu keine Vorgaben auf.

Beispielsweise können durch Verhaltensregeln die faire und transparente Verarbeitung (Art. 40 Abs. 2 lit. a), die berechtigten Interessen des Verantwortlichen in bestimmten Zusammenhängen (lit. b), die Erhebung personenbezogener Daten (lit. c), die Ausübung der Rechte der betroffenen Personen (lit. f) und die Maßnahmen und Verfahren gemäß den Artikeln 24 und 25 und die Maßnahmen für die Sicherheit der Verarbeitung nach Art. 32 (lit. h) näher geregelt werden. Nach ErwG. 98 DSGVO soll dabei stets den besonderen Bedürfnissen der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen Rechnung getragen werden.[2]

1 Download möglich unter: www.inkasso.de/positionen/standpunkte/best-practice-guide-dsgvo.

2 Einen dezidierten Überblick zu Verhaltensregeln nach Art. 40 DSGVO sowie deren Reichweite und Rechtsfolgen gibt *Spindler* in ZD 2016, Selbstregulierung und Zertifizierungsverfahren nach der DSGVO, 407.

© Copyright Erich Schmidt Verlag GmbH & Co. KG, Berlin 2017 - (http://www.pingdigital.de) 11.07.2017 - 08:27

Lizenziert für Frau Daniela Gaub.
Die Inhalte sind urheberrechtlich geschützt.

Nähere und vor allem für alle einheitliche Hinweise und Beispiele sind nach weitverbreiteter Einschätzung tatsächlich besonders hilfreich für die Kleinst-, kleinen und mittleren Unternehmen.

Aufgrund der Struktur der Mitgliedsunternehmen des BDIU gab es daher zunächst bei diesem Überlegungen, Verhaltensregeln im Sinne der DSGVO auszuarbeiten. Grundsätzlich wurden und werden diese immer noch als sinnvoll erachtet, denn Regeln und Verfahren im Rahmen einer freiwilligen Selbstbindung aus einer Branche heraus sind sicherlich mehr wert als abstrakt-generelle Regelungen. Sie können sowohl dem Anwender als auch der Aufsicht einen detaillierteren Einblick in einzelne Abläufe und die Besonderheiten einer Branche gewähren.

2. Gründe gegen Verhaltensregeln auf nationaler Ebene für den Bereich Forderungsmanagement

Ein maßgeblicher Grund, warum der BDIU nun aber doch von der Erstellung von Verhaltensregeln abgesehen hat, liegt an Art. 40 Abs. 5 DSGVO, der explizit eine Einbeziehung der nach Art. 55 DSGVO zuständigen Aufsichtsbehörde erfordert.

Dass die bzw. der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) die Aufsichtsbehörde in Deutschland ist, die die Aufgaben nach Art. 57 DSGVO wahrnimmt, steht jedoch erst seit Kurzem fest.[3] Verhaltensregeln für (ausschließlich) in Deutschland ansässige datenverarbeitende Unternehmen können also – möchte man das in der DSGVO vorgegebene Verfahren einhalten – faktisch erst jetzt in Kollaboration mit der bzw. dem BfDI ausgearbeitet werden.

In Anbetracht der vielfältigen Aufgaben der bzw. des BfDI allein bis zum Anwendungsbeginn der DSGVO rechnete der BDIU nicht mit einem schnellen Abstimmungsprozess, selbst wenn die Aufsichtsbehörde gemäß DSGVO dazu angehalten ist, die Ausarbeitung von Verhaltensregeln zu fördern.

Ein weiterer Grund, warum sich der BDIU zum jetzigen Zeitpunkt gegen nationale Verhaltensregeln für den Bereich Forderungsmanagement ausgesprochen hat, liegt darin, dass der europäische Dachverband, die Federation of European National Collection Associations (FENCA),[4] die Ausarbeitung von Verhaltensregeln beschlossen hat. Der Code of Conduct[5] wird dabei nach den Vorgaben des Art. 40 DSGVO erstellt werden und soll europaweit für den Bereich des Forderungsmanagements gelten.[6] Blickt man auf das Ziel der DSGVO, das Datenschutzrecht europaweit vereinheitlichen zu wollen, ist die Erstellung von ebenso europaweit einheitlichen Präzisierungen zur Anwendung der Verordnung folgerichtig.

Da also zum einen auf nationaler Ebene bislang nicht klar war, mit welcher Aufsichtsbehörde die Abstimmung nach Art. 40 Abs. 5 DSGVO erfolgen soll, zum anderen die paneuropäischen Verhaltensregeln der FENCA erwartet werden, entschied sich der BDIU im Frühsommer 2016 für einen anderen Weg – die Ausarbeitung eines Best Practice Guides.

III. Best Practice Guide – Inhalt und Entwicklung

Die Idee dahinter war es, den Unternehmen der Branche und weiteren Tätigen im Bereich des Forderungsmanagements einen Leitfaden an die Hand geben zu wollen, aus dem in ersten Grundzügen hervorgeht, wie bis Mai 2018 die Datenverarbeitungen konform mit den neuen DSGVO-Anforderungen ausgestaltet werden sollten.

Die Anpassung der Prozessabläufe und die weitere Implementierung der DSGVO-Vorgaben, v. a. was die Dokumentationsanforderungen anbelangt, kann nämlich nicht von heute auf morgen geschehen, sodass eine zügige erste Hilfestellung unabdingbar war. Der Best Practice Guide wurde daher schnellstmöglich erstellt und war Anfang 2017 fertiggestellt.

1. Inhalt

Die 41 Seiten umfassende Handlungsempfehlung des BDIU beginnt mit einem Vorwort der BDIU-Präsidentin *Kirsten Pedd*, mit dem bereits klar wird, dass der Best Practice Guide ein wirkliches Hilfsmittel für die Unternehmen der Branche sein soll.

Da sich aber sicherlich nicht alle Adressaten des Best Practice Guides mit europäischen Gesetzgebungsverfahren auskennen, wird als eigentlicher Beginn des BDIU-Leitfadens zunächst ein Kurzüberblick dazu gegeben, was die Regelung in Form einer europäischen Verordnung bedeutet und im Weiteren – auch zum besseren Verständnis für die weitere Lektüre – die wichtigsten Begriffe der DSGVO vorgestellt, dies bereits mit branchenrelevanten Erläuterungen.

Danach folgt der eigentliche Inhalt: Die DSGVO-Regelungen zu den Grundlagen der Datenverarbeitung, die Informationspflichten und die Betroffenenrechte werden beleuchtet. Dabei werden stets für den Bereich des Forderungsmanagements einschlägige Beispiele aufgeführt und aufgezeigt, Besonderheiten herausgehoben und hilfreiche Tipps für die Praxis gegeben. In gleicher Weise werden v. a. die Anforderungen an die Dokumentation, der sichere Umgang mit Daten durch technisch-organisatorische Maßnahmen, die Stellung des betrieblichen Datenschutzbeauftragten, die Auftragsverarbeitung, mögliche Sanktionen und die Tätigkeit der Aufsicht in den Blick genommen.

Der Leitfaden endet schließlich mit einem Katalog der für Inkassodienstleister maßgeblichen Begriffsbestimmungen sowie einer Synopse, die die einzelnen Artikel der DSGVO den jeweils passenden Erwägungsgründen gegenüberstellt.

2. Entwicklung

Der Weg bis zur Druckfassung des Leitfadens war zwar – im Vergleich zu manch anderen Druckerzeugnissen – nicht lang: Den Startschuss gab es im Frühsommer 2016. Anfang Februar 2017 wurde der Best Practice Guide veröffentlicht.

Dennoch: die Entwicklungsphase von guten acht Monaten war mehr als intensiv und bedeutete für alle Beteiligten eine nicht zu unterschätzende Zusatzbelastung. Wenn man sich genau anschaut, wer an der Erstellung mitgewirkt hat, wird schnell klar, dass es nicht als selbstverständlich angesehen werden kann, dass in dieser Zeit ein Werk dieses Umfangs und dieser Qualität entstehen kann.

Auch wenn der BDIU mit seinen hauptamtlichen Mitarbeitern mit am Werk war, wurde der Inhalt zum Großteil von Praktikern beigesteuert. So haben alle Mitglieder des BDIU-Datenschutzausschusses, die in dieser Position ehrenamtlich und damit neben ihrer eigentlich Tätigkeit (zumeist als Datenschutzbeauftragte in den oder für Inkassounternehmen) tätig sind, an der Erstellung mitgewirkt. Auch der Verbandsbeauftragte für den Datenschutz des BDIU hat bei der Entwicklung des Leitfadens seine Expertise eingebracht.

Nach Verteilung einzelner Themenbereiche durch die BDIU-Geschäftsstelle hat sich jeder der Beteiligten an die Ausarbeitung seines Parts gemacht und nahm die jeweiligen DSGVO-Regelungen aus Praxissicht in den Blick. Die innerhalb einer gesetzten Frist übersandten Manuskripte der Einzelnen hat die BDIU-Geschäftsstelle anschließend zusammengefügt und bereits eine erste sprachliche Anpassung vorgenommen. Bei einem ersten Treffen gut zweieinhalb Monate nach der Themenvergabe wurde in einem Arbeitstreffen des

3 Der Bundestag hat das BDSG-neu als Bestandteil des DSAnpUG-EU (BT-Drs. 18/11325) am 27. April 2017 in der Fassung der Beschlussempfehlung des Innenausschusses (BT-Drs. 18/12084) verabschiedet. Der Bundesrat hat am 12. Mai 2017 dem Gesetz zugestimmt.

4 Der BDIU ist Gründungsmitglied der FENCA.

5 In der englischen Sprachfassung der DSGVO werden die Verhaltensregeln in Art. 40 mit Codes of Conduct bezeichnet.

6 FENCA-News zum Code of Conduct: http://fenca.eu/detail/article/fenca-is-working-on-a-pan-european-code-of-conduct/.

© Copyright Erich Schmidt Verlag GmbH & Co. KG, Berlin 2017 - (http://www.pingdigital.de) 11.07.2017 - 08:27

Lizenziert für Frau Daniela Gaub.
Die Inhalte sind urheberrechtlich geschützt.

BDIU-Datenschutzausschusses der erste Teil des Manuskripts besprochen und dezidiert über jedes einzelne Kapitel diskutiert, bis zu allen Punkten Einigkeit herrschte. Die BDIU-Geschäftsstelle passte das Manuskript im Nachgang entsprechend der Ergebnisse des Arbeitstreffens an. Das gleiche Vorgehen erfolgte bezüglich der noch verbleibenden Teile bei weiteren Arbeitstreffen bzw. regulären Ausschusssitzungen, bis Anfang Dezember 2016 die finale Ausarbeitung der Verfasser auf dem Tisch lag.

Um die Lesbarkeit und damit das Verständnis auch für die Leser zu gewährleisten, die sich bislang noch nicht intensiv mit dem Datenschutzrecht auseinandergesetzt haben, erfolgte noch von externer Seite eine sprachliche Überarbeitung des Best Practice Guides. Im Folgenden musste noch ein letzter Abgleich zwischen der ursprünglichen Finalfassung und der Fassung nach der sprachlichen Überarbeitung stattfinden, um sicherzugehen, dass trotz der Überarbeitung die inhaltlichen Aussagen gleichgeblieben waren.

Schließlich stimmte die BDIU-Geschäftsstelle mit einer beauftragten Agentur das Layout des Best Practice Guides ab, bevor dieser dann in der Printfassung an die Mitglieder des BDIU versandt, als (kostenfrei) downloadbares PDF auf die Verbandshomepage gestellt und beim BDIU-Kongress am 7. April 2017 im Rahmen eines Workshops vorgestellt wurde.[7] Bei dieser Gelegenheit war es bereits möglich, erste Fragen zum Best Practice Guide bzw. zur Anwendbarkeit der DSGVO zu stellen.

IV. Ausblick

In den kommenden Monaten wird der BDIU auch noch näher den Inhalt des Best Practice Guides bei den Sitzungen der regionalen Arbeitskreise des Verbandes vorstellen und den dortigen Teilnehmern Rede und Antwort zu datenschutzrechtlichen Fragen stehen.

Bis zum Anwendungsbeginn der DSGVO wird der BDIU seinen Mitgliedern zudem regelmäßig Factsheets zur Verfügung stellen, aus denen für die Unternehmen vertiefende, dabei prägnante Erläuterungen und Tipps zu einzelnen Themen der DSGVO hervorgehen, bestenfalls auch bereits erste Anwendungshinweise der Datenschutzaufsichtsbehörden.

Der Titel „Best Practice Guide 1.0 – Leitfaden für den Bereich Forderungsmanagement“ lässt es ansonsten bereits erkennen, dass er und der Umgang mit der DSGVO „work in progress“ sind. So berücksichtigt der Leitfaden noch nicht die Regelungen des deutschen BDSG-neu, das als Bestandteil des DSAnpUG-EU bereits beschlossen wurde,[8] sondern nur die DSGVO-Regelungen. Es sind schon allein deshalb noch genügend Fragen offen, zu denen es sicherlich zu gegebener Zeit noch Antworten geben wird – vielleicht in einem „Best Practice Guide 2.0“ ...

7 Siehe Fußnote 1.

8 Siehe Fußnote 3.

© Copyright Erich Schmidt Verlag GmbH & Co. KG, Berlin 2017 - (http://www.pingdigital.de) 11.07.2017 - 08:27