LEITFADEN

Umsetzung der EU-Datenschutz-Grundverordnung

Leitfaden für Auftragsverarbeiter

Autor:
Rechtsanwalt Ulrich Meyer, Gettorf
für Dataport, AöR

Vitako-Arbeitskreis:
Korinna Pöppl, AKDB
Holger Brinkmeyer, ITEBO
Kim Schoen, ITEBO
Christoph Ludwig, DVV Baden-Württemberg
Frank Fricke, Stadt Köln
Uwe Wunsch, Lecos GmbH

Datum: Februar 2018

VITAKO
Bundes-Arbeitsgemeinschaft der
Kommunalen IT-Dienstleister e.V.

VITAKO
Bundes-Arbeitsgemeinschaft der
Kommunalen IT-Dienstleister e.V.

Inhaltsverzeichnis

1	Zielsetzung	3
2	Vertragliche Ausgestaltung des Auftragsverhältnisses	4
3	Anforderungen an Auftragsverarbeiter	6
4	Einsatz von Unterauftragnehmern	7
5	Fernwartung	8
6	Technische und organisatorische Maßnahmen	9
7	Nachweis- und Kontrollpflichten	9
8	Unterstützung des Verantwortlichen	10
9	Haftung	10
10	Aufsichtsbehörden	11
11	Datenschutzbeauftragter	12
12	Verzeichnis von Verarbeitungstätigkeiten	13
13	Weiterführende Informationen	14

1 Zielsetzung

Ab 25. Mai 2018 müssen alle privaten und öffentlichen Organisationen, die personenbezogene Daten verarbeiten, die Anforderungen der europäischen Datenschutz-Grundverordnung (DSGVO) erfüllen. Diese Pflicht trifft ohne Ausnahme auch die in der Bundesarbeitsgemeinschaft Vitako organisierten kommunalen IT-Dienstleister. Auch für sie stellt sich deshalb die Frage, welche Veränderungen das neue Datenschutzrecht mit sich bringt und wie diesem bezogen auf das originäre Aufgabenportfolio in rechtlicher, technisch-organisatorischer und vertraglicher Sicht zu begegnen ist.

Dieser Leitfaden soll ausgehend von der neuen europäischen und ergänzenden deutschen Rechtslage auf Bundes- und Länderebene aufzeigen, an welchen Stellen am vorhandenen Regelwerk Änderungen, Ergänzungen oder Streichungen in den jeweiligen Häusern vorzunehmen sind. Diverse bereits veröffentlichte Leitfäden befassen sich mit generellen Themen entlang der gesamten Breite der DSGVO. **Dieser Leitfaden fokussiert daher auf den für IT-Dienstleister besonders wichtigen Bereich der Auftragsverarbeitung.** Neben der Darstellung und Erläuterung der einschlägigen Bestimmungen der Verordnung zeigt er **Möglichkeiten zur rechtskonformen Umsetzung der Anforderungen auf, die auf praktischen Erfahrungen basieren**.

Die DSGVO hat den Rechtscharakter einer europäischen Verordnung. Sie entfaltet deshalb im Gegensatz zu einer Richtlinie unmittelbare Gesetzeskraft für alle Mitgliedsstaaten. Sie erlaubt den nationalen Gesetzgebern ergänzende oder konkretisierende eigene Regelungen. Dabei bleibt aber der Erlass identischer nationaler Regelungen ebenso verboten wie Abweichungen von dem von der DSGVO postulierten Datenschutzniveau (Wiederholungs- und Verschärfungsverbot). In Konsequenz dessen müssen in Deutschland das Bundesdatenschutzgesetz (BDSG) und alle Landesgesetze mit Datenschutzbezug angepasst werden. Dieser Prozess ist bisher (Stand Februar 2018) nicht abgeschlossen. Diese Tatsache steht aber der Entfaltung von Aktivitäten mit Blickrichtung auf den nahenden Stichtag Ende Mai dieses Jahres nicht im Weg. Denn Aufgrund der bestehenden Gesetzeshierarchie mit der DSGVO an der Spitze reicht es zunächst aus, diesen Leitfaden auf die Verordnung zu beziehen. Es ist nicht damit zu rechnen, dass für IT-Dienstleister, die sich entsprechend der DSGVO aufstellen, ein nennenswerter zusätzlicher Nachbesserungsaufwand durch noch zu erlassende landesspezifische Regelungen entstehen wird.

2 Vertragliche Ausgestaltung des Auftragsverhältnisses

Durch die DSGVO werden **neue Terminologien** vorgegeben, die auch im folgenden Text verwendet werden.

- Die ehemals „datenverarbeitende Stelle“ wird zum „Verantwortlichen“. „Verantwortlicher“ ist gemäß Art. 4 Nr. 7 DSGVO die „natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet“.
- Die „Auftragsdatenverarbeitung“ oder „Datenverarbeitung im Auftrag“ wird zur „Auftragsverarbeitung“ und
- der Auftragnehmer einer Datenverarbeitung wird gemäß Art. 4 Nr. 8 DSGVO zum „Auftragsverarbeiter“.

Die Auftragsverarbeitung darf gemäß Art. 28 Abs. 3 DSGVO nur Aufgrundlage eines Vertrages oder eines „anderen Rechtsinstruments […], das den Auftragsverarbeiter […] bindet“, erfolgen. Die nicht-vertragliche Bindung könnte sich aus einem Subordinationsverhältnis zwischen Verantwortlichem und Auftragsverarbeiter ergeben. Wenn etwa der Auftragsverarbeiter dem vollen fachlichen Weisungsrecht des Verantwortlichen unterliegt, oder der Verantwortliche qua Satzung dem Auftragsverarbeiter verpflichtende Vorgaben machen kann, wäre auch das konform mit Art. 28 DSGVO, sofern die sonstigen Vorgaben erfüllt sind. In beiden Fällen (Vertrag oder sonstiges Institut) müssen nämlich Gegenstand, Dauer, Art und Zweck der Verarbeitung, Art der personenbezogenen Daten und Kategorien betroffener Personen sowie Rechte und Pflichten des Verantwortlichen festlegt sein. Derartige Verträge sind auch nach derzeitigem Recht schon unabdingbar, so dass deren Existenz vorausgesetzt werden kann. **Anders als im bisherigen Recht enthält die DSGVO aber teilweise konkretere Vorgaben über die Breite der zu treffenden Vereinbarung. Es ist deshalb notwendig, bestehende Verträge darauf zu prüfen, ob die von der DSGVO geforderten Festlegungen bereits darin berücksichtigt sind.** In Abhängigkeit vom Prüfungsergebnis werden Änderungen und Ergänzungen erforderlich oder angezeigt sein. Gegebenenfalls kann die zum Stichtag zwingende Umsetzung der DSGVO auch zum Anlass genommen werden, Verträge über das Auftragsverhältnis gänzlich neu zu fassen. Vielfach sind Verträge durch Änderungen und Anpassungen über längere Zeiträume unübersichtlich und dadurch schwerer verständlich geworden. Der Aufwand für redaktionelle und strukturelle Überarbeitungen und die dafür erforderlichen Abstimmungen mit den Auftraggebern wurde aus nachvollziehbaren Gründen gescheut. Die DSGVO könnte in diesen Fällen auch mit Blick auf die Kommunikation mit Auftraggebern Anlass für eine Neufassung der Verträge zur Auftragsverarbeitung sein.

Die Überprüfung der bestehenden Verträge erfolgt zweckmäßigerweise entlang des Kataloges aus Art. 28 Abs. 3 DSGVO und umfasst deshalb die folgenden Punkte:

a) Enthält der Vertrag eine Bestimmung, wonach der Auftragsverarbeiter nur aufgrund dokumentierter Weisung tätig werden darf? Wird der Auftragsverarbeiter zur Mitteilung vor Beginn der Verarbeitung verpflichtet, dass er nach dem für ihn geltenden Recht der Union oder der Mitgliedsstaaten zur Übermittlung personenbezogener Daten an ein Drittland oder an eine internationale Organisation verpflichtet ist?

b) Ergibt sich aus dem Vertrag, dass die Mitarbeiter des Auftragsverarbeiters zur Verschwiegenheit zu verpflichten sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen?

c) Enthält der Vertrag die Verpflichtung des Auftragsverarbeiters zur Gewährleistung der Sicherheit der Verarbeitung gemäß Art. 32 DSGVO?

d) Ist die Erteilung von Unteraufträgen entsprechend Art. 28 Abs. 2 und 4 DSGVO geregelt?

e) Enthält der Vertrag die Verpflichtung des Auftragsverarbeiters, die verantwortliche Stelle bei der Wahrnehmung ihrer Pflichten gegenüber betroffenen Personen zu unterstützen?

f) Enthält der Vertrag die Verpflichtung des Auftragsverarbeiters, die verantwortliche Stelle bei der Wahrnehmung ihrer Pflichten zur Wahrung der Sicherheit der Datenverarbeitung zu unterstützen?

g) Ist die Rückgabe von überlassenen Daten und Verarbeitungsergebnissen oder deren Löschung nach Beendigung des Auftragsverhältnisses geregelt?

h) Enthält der Vertrag die Verpflichtung des Auftragsverarbeiters, der verantwortlichen Stelle Nachweise über die Erfüllung der Anforderungen aus Art. 28 DSGVO zur Verfügung zu stellen und Kontrollen durch den Verantwortlichen oder einen beauftragten Prüfer zu ermöglichen?

Anmerkungen zum Katalog aus Art. 28 Abs. 3 DSGVO:

zu a) Die Weisungsgebundenheit wird in allen bisherigen Verträgen enthalten sein, Bestimmungen zu Verarbeitungen in Drittländern jedoch nicht. Sofern Dienstleister Verfahren in Rechenzentren von Drittländern durch Provider hosten lassen oder Cloud-Dienste von außereuropäischen Providern in Anspruch nehmen, müssen die Verträge entsprechend angepasst werden. Dabei ist damit zu rechnen, dass die verantwortlichen Stellen dies kritisch sehen und ein höherer Abstimmungsaufwand entsteht.

Der Aspekt, personenbezogene Daten ohne entsprechende Weisung zu verarbeiten, weil dazu eine gesetzliche Verpflichtung besteht, kann vernachlässigt werden. Im Tätigkeitsbereich der Vitako-Dienstleister sind keine diesbezüglichen Verpflichtungen erkennbar.

zu b) Entsprechende Bestimmungen sollten in den bereits bestehenden Verträgen zwischen Verantwortlichen und Auftragsverarbeitern enthalten sein.

zu c) Unabhängig davon, wie die technischen und organisatorischen Maßnahmen tatsächlich ausgestaltet und in den vorhandenen Verträgen unmittelbar oder in Vertragsbestandteilen dargestellt sind, ist eine Umstellung auf die Garantien des Art. 28 DSGVO erforderlich. Außerdem muss die Einhaltung des Sicherheitskonzepts nach Art. 32 DSGVO einschließlich der Evaluation und Fortschreibung nach dem Stand der Technik aufgenommen werden. Eine Anpassung bestehender Verträge ist erforderlich.

zu d) Da die Voraussetzungen für den Einsatz von Unterauftragnehmern (weitere Auftragsverarbeiter) enger und konkreter gefasst sind als bisher, müssen bestehende Verträge angepasst werden.

zu e) Die DSGVO enthält neue Rechte für Betroffene, insbesondere das „Recht auf Vergessenwerden“, also das Recht auf Löschung. Entsprechende Unterstützungspflichten des Auftraggebers müssen aufgenommen werden.

zu f) Bei den referenzierten Bestimmungen handelt es sich um gesetzliche Verpflichtungen des Verantwortlichen und des Auftragsverarbeiters. Sofern es sich nicht um unmittelbare Pflichten des Auftragsverarbeiters handelt (zum Beispiel unverzügliche Mitteilung von Datenschutzverstößen an den Verantwortlichen) ist der Verantwortliche auf Unterstützung durch den Auftragsverarbeiter angewiesen. Dazu muss sich dieser vertraglich verpflichten – was in vielen der bisherigen Verträge vermutlich nicht vorgesehen war.

3 Anforderungen an Auftragsverarbeiter

Art. 28 DSGVO ist die zentrale Norm für die Auftragsverarbeitung. Ihr Inhalt zielt insgesamt in dieselbe Richtung wie die entsprechenden Vorschriften im Bundesdatenschutzgesetze (BDSG) sowie der sechzehn Landesdatenschutzgesetze (LDSG), auch wenn deren Fassungen noch nicht durchgängig mit Blick auf die DSGVO novelliert wurden und die Formulierungen nicht wortgleich zur DSGVO sind.

Insofern enthält Art. 28 Abs. 1 DSGVO zwar keine ganz neuartigen Anforderungen, aber klarstellende Konkretisierungen der schon jetzt durch Bundes- und Landesgesetzgebung bestehenden Forderung nach „sorgfältiger Auswahl“ des Auftragnehmers. **Das bedeutet, dass ein IT-Dienstleister, der nach derzeitigem Recht als „sorgfältig ausgewählt“ gelten kann, im Prinzip auch den Anforderungen der DSGVO entspricht. Dabei ist allerdings zu beachten, dass in der DSGVO mehr als bisher darauf abgestellt wird, dass er „hinreichende Garantien“ für die Umsetzung technischer und organisatorischer Maßnahmen bieten muss, die die datenschutzkonforme Verarbeitung personenbezogener Daten Betroffener gewährleisten.** Die „hinreichende Garantie“ ist ein unbestimmter Rechtsbegriff, der durch vertragliche Regeln entsprechend den Vorgaben der DSGVO konkretisiert werden muss.

Hinreichende Garantien können zum Beispiel gewährt werden durch

- Zertifizierungen auf Grundlage anerkannter Standards wie BSI-Grundschutz oder ISO 27001,
- Ergebnisse eines Selbstaudits, durch genehmigte Verhaltensregeln (Art. 40 DSGVO) oder
- verbindliche interne Datenschutzvorschriften (Art. 47 DSGVO).

Im zweit- und drittgenannten Fall – Selbstaudit und Anwendung verbindlicher interner Datenschutzvorschriften – sind **externe Nachweise über die Einhaltung dieser hinreichenden Garantien notwendig**. Dies können zum Beispiel Zertifikate gemäß Art. 42 DSGVO sowie ein aktuelles Testat und/oder Berichte oder Berichtsauszüge unabhängiger Instanzen (etwa Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) sein.

Der Auftragsverarbeiter ist dafür gegenüber dem Verantwortlichen nachweispflichtig. In der Folge werden sich die Anforderungen an Qualität und Umfang (der Datenschutz- und Sicherheitsdokumentation) zum Erreichen von DSGVO-Konformität erhöhen.

4 Einsatz von Unterauftragnehmern

Art. 28 Abs. 2 macht die Erteilung von Unteraufträgen von der vorherigen schriftlichen Genehmigung des Auftraggebers (der verantwortlichen Stelle) abhängig. Dies ist gegenüber dem geltenden Recht im Grundsatz keine neue Forderung. **In der DSGVO wird aber explizit kodifiziert, dass an die Vereinbarungen mit Unterauftragnehmern ausdrücklich dieselben inhaltlichen Anforderungen gestellt werden wie an die Vereinbarung zwischen verantwortlicher**

Stelle und Auftragsverarbeiter selbst (Art. 28 Abs. 4 DSGVO). **Daraus folgt eine Nachweispflicht, die es in dieser Form bisher nicht gab.** Die Vereinbarung zwischen Verantwortlichen und Auftragsverarbeitern enthält unter Anderem konkrete Zusicherungen des Auftragsverarbeiters über technische und organisatorische Maßnahmen zur Datensicherheit und Kontrollrechte und -pflichten der verantwortlichen Stelle. Als Folge aus Art. 28 Abs. 4 DSGVO müssen diese Maßnahmen und Kontrollrechte in einer lückenlosen Kette bis zum letzten Unterauftragnehmer weitergereicht werden. Schließlich begründet die Vorschrift die Haftung des ersten Auftragsverarbeiters auch für Datenschutzverletzungen der Nachauftragnehmer. Deshalb erfordern die Unterauftragsverhältnisse künftig eine erhöhte Aufmerksamkeit und es entsteht Handlungsbedarf.

Bei Unterauftragsverhältnissen wird der Auftragsverarbeiter zum Auftraggeber des Unterauftragnehmers. Das hat zur Folge, dass er in die Verantwortung für die ordnungsgemäße vertragliche Ausgestaltung kommt und dass er auch die Haftung für weitere Auftragsverarbeiter übernimmt und sie wirksam kontrollieren muss. Entsprechende Verträge müssen spätestens am 25. Mai 2018 abgeschlossen sein. Das bedeutet, dass bis dahin auch ein Kontrollkonzept (Lieferantenaudit) zu erstellen ist. Wegen der Mitwirkungspflicht der verantwortlichen Stelle beim Wechsel von nur allgemein genehmigter Unterauftragsverarbeitung (Widerspruchsrecht) müssen auch dafür Prozesse aufgesetzt werden. Der Handlungsbedarf hängt davon ab, ob und wie konkret die derzeitigen Vereinbarungen mit Unterauftragnehmern vertraglich schriftlich geregelt sind.
Auf jeden Fall sind folgende Punkte zu prüfen:

- Ist der Einsatz von Unterauftragsverarbeitern im Kundenvertrag DSGVO-konform geregelt?
- Gibt es ein Konzept oder einen dokumentierten Prozess zur Kontrolle des Unterauftragsverarbeiters?
- Gibt es ein Change-Management für Unterauftragsverhältnisse unter Einbeziehung des jeweiligen Verantwortlichen? Das umfasst den Prozess der Identifikation der Kunden, für die ein konkreter Unterauftragsverarbeiter relevant ist, die Kommunikation mit dem Kunden über den beabsichtigten Wechsel des Unterauftragsverarbeiters und die Genehmigung oder Verweigerung des Verantwortlichen.

5 Fernwartung

Den vorangegangenen Aussagen kommt besondere Beachtung zu, wenn Auftragsverarbeiter andere Dienstleister mit Support- und Fernwartungsaufgaben betrauen. Sofern es sich hierbei nicht um rein technische Wartung der Infrastruktur wie beispielsweise Arbeiten an Elektroinstallationen, Heizungs- oder

Klimaanlagen, sondern um Arbeiten an Hard- und Software mit der Notwendigkeit oder zumindest der Möglichkeit des Zugriffs auf personenbezogene Daten handelt, wird dies aufgrund der weiten Definition der „Verarbeitung“ in Art. 4 Nr. 2 DSGVO als Form einer Auftragsverarbeitung zu sehen sein. Infolgedessen gelten die Anforderungen, die an die Auswahl des Auftragsverarbeiters gestellt werden – die vertragliche Ausgestaltung, Haftung und Kontrolle – in gleichem Maße wie bei anderen Auftragsverarbeitungsverhältnissen. **Diesem Aspekt wurde in der Vergangenheit sicher bereits bei Zertifizierungen Rechnung getragen. Er wird künftig jedoch besonders genau zu betrachten sein, wenn Fernwartungstätigkeiten aus Drittländern erfolgen sollen oder aufgrund der Organisation des Dienstleisters die Möglichkeit dazu besteht.** Hier wird besonders auf DSGVO-konforme Ausgestaltung des Konstrukts und dessen Überwachung durch den als Verantwortlichen agierenden Auftragsverarbeiter zu achten sein.

6 Technische und organisatorische Maßnahmen

Die im bisherigen Recht mit gleicher Zielrichtung, aber unterschiedlichen Formulierungen in der Anlage zu §9 BDSG und den Landesdatenschutzgesetzen festgelegten technischen und organisatorischen Maßnahmen (TOM) zur Sicherheit der Datenverarbeitung finden sich in Art. 32 DSGVO. Diese Norm zielt auf die bekannten Schutzziele „Sicherheit“, „Vertraulichkeit“, „Integrität“ und „Verfügbarkeit“ sowie zusätzlich „Belastbarkeit“. Hinsichtlich dieser Ziele sind technische und organisatorische Maßnahmen zu treffen, die ein dem Risiko angemessenes Schutzniveau gewährleisten und den Stand der Technik und die Implementierungskosten berücksichtigen. Im Prinzip tritt hier durch die DSGVO keine materielle Änderung ein.

7 Nachweis- und Kontrollpflichten

Anders als im bisherigen Recht trifft die Verantwortlichen eine Rechenschaftspflicht hinsichtlich der Einhaltung der Grundsätze für die Verarbeitung personenbezogener Daten gemäß Art. 5 DSGVO. Der Gesetzgeber fordert in Art. 5 Abs. 2 DSGVO wörtlich, dass der Verantwortliche die Einhaltung der dort genannten Datenschutzgrundsätze nachweisen können muss. Diese Anforderung gilt unmittelbar nur für den Verantwortlichen und nicht für den Auftragsverarbeiter. **Der Auftragsverarbeiter ist allerdings nach Art. 38 Abs. 3 lit. h gehalten, dem Verantwortlichen die erforderlichen Nachweise über die Einhaltung seiner Pflichten zur Verfügung zu stellen und Überprüfungen (Kontrollen) zu dulden und aktiv zu unterstützen.** Diese Nachweise können zum Beispiel durch

erfolgreich abgeschlossene Zertifizierungen erbracht werden (s.o. im Abschnitt „Anforderungen an Auftragsverarbeiter“).

8 Unterstützung des Verantwortlichen

Im Zusammenhang mit den zu treffenden technischen und organisatorischen Maßnahmen und den Nachweis- und Kontrollpflichten, für die die verantwortliche Stelle – die Behörden- oder Unternehmensleitung – verantwortlich ist, gibt es auch Erwartungen an Unterstützung durch den dienstleistenden Auftragsverarbeiter. Das Institut der Auftragsverarbeitung erlaubt den Beteiligten die Konzentration auf deren jeweilige Kernkompetenz: Verwaltung und Geschäftsprozesse auf der einen, IT-, technisches und betriebstechnisches Know-how auf der anderen Seite. Gerade für kleinere Verwaltungseinheiten ist das Outsourcing der IT einschließlich Infrastruktur und Fachanwendungen unter wirtschaftlichen Gesichtspunkten unerlässlich. Ungeachtet dessen bleibt der Verantwortliche in der Verantwortung für die Sicherheit und Ordnungsmäßigkeit der Verarbeitung personenbezogener Daten der Bürgerinnen und Bürger. **Das kann nur funktionieren, wenn der Auftragsverarbeiter dafür Sorge trägt, dass die „richtigen“ technischen und organisatorischen Maßnahmen zum Gegenstand seiner vertraglichen Bindung gemacht werden. Auftragsverarbeiter müssen ihre Auftraggeber entsprechend beraten und sie vor allem auch mit der gebotenen Transparenz über die Maßnahmen, ihre Wirksamkeit und ihre Kontrolle informieren.** Diese Beratung kann zum eigenständigen Angebot entwickelt werden. Besonderes Interesse dürfte daran bestehen, wenn technische und organisatorische Maßnahmen auch bereits in der Sphäre des Verantwortlichen zu treffen sind.

9 Haftung

Jede Person, der wegen eines Verstoßes gegen die Datenschutz-Grundverordnung ein materieller oder immaterieller Schaden entstanden ist, hat nach Art. 82 Abs. 1 DSGVO Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter. Für einen Auftragsverarbeiter gilt die Einschränkung gemäß Art. 82 Abs. 2 DSGVO, dass er nur dann für den durch eine Verarbeitung verursachten Schaden haftet, wenn er seinen speziell den Auftragsverarbeitern auferlegten Pflichten aus dieser Verordnung nicht nachgekommen ist oder unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des für die Datenverarbeitung Verantwortlichen oder gegen diese Anweisungen gehandelt hat. Die Haftung für Datenschutzverstöße ist verschuldensabhängig. Verantwortlicher und Auftragsverarbeiter können sich gemäß Art. 82 Abs. 3 DSGVO von der Schuld befreien, wenn sie nachweisen, dass sie in

keiner Weise für den entstandenen Schaden verantwortlich sind. Mehrere an der Verarbeitung Beteiligte einschließlich der Kombination „Verantwortlicher“ und „Auftragsverarbeiter“ haften bei Verstößen, die ihnen zuzuordnen sind, gesamtschuldnerisch, sofern sie sich nicht von der Schuld befreien konnten. Gesamtschuldnerische Haftung bedeutet, dass der Geschädigte seinen gesamten Schaden gegenüber jedem der Beteiligten geltend machen kann, insgesamt allerdings nur einmal. Er hat aber ein Wahlrecht, gegen das sich der in Anspruch Genommene nicht wehren kann. Der in Anspruch Genommene hat gegen die Mitbeteiligten einen Ausgleichsanspruch, trägt aber das Risiko, diesen möglicherweise nicht realisieren zu können. **Diese Haftungsproblematik ist bei der Bewertung des wirtschaftlichen Risikos des Auftragsverarbeiters, für IT-Dienstleister des Unterauftragsverarbeiters zu berücksichtigen.**

10 Aufsichtsbehörden

Aufgrund der Regelung in Art. 51 DSGVO und des Erwägungsgrundes 117, wonach die Mitgliedstaaten mehr als eine Aufsichtsbehörde errichten können, wenn dies ihrer verfassungsmäßigen, organisatorischen und administrativen Struktur entspricht, wird es für die Bundesrepublik Deutschland bei der bisherigen Konstellation mit einem Bundesdatenschutzbeauftragten und den Landesdatenschutzbeauftragten bleiben. Das Bundesdatenschutzgesetz wurde inzwischen angepasst, auf Länderebene laufen Novellierungsverfahren.
Die Aufsichtsbehörden haben wie bisher in unterschiedlichen Ausprägungen gegenüber Verantwortlichen und Auftragsverarbeitern Untersuchungs- (= Prüfungs-) und Abhilfebefugnisse (Art. 58 Abs. 1 und 2 DSGVO). Werden bei Untersuchungen Verstöße oder zu vermutende Verstöße festgestellt, kommen die Abhilfebefugnisse nach Artikel 58 Abs. 2 in drei verschiedene Stufen zur Anwendung:

a) Warnungen (Art. 58 Abs. 2 lit. a, b)

b) Anweisungs- und Anordnungsbefugnisse (Art. 58 Abs. 2 lit. c, d, e, g, h)

c) Sanktionsbefugnisse (Art. 58 Abs. 2 lit. f, h, i, j)

Die Sanktionsbefugnisse können neben Verantwortliche auch IT-Dienstleister als Auftragsverarbeiter treffen. Dabei ist davon auszugehen, dass die Sanktionen von den Aufsichtsbehörden als „ultima ratio“ nur dann ausgesprochen werden, wenn absehbar ist, dass mildere Mittel nicht greifen beziehungsweise durch Nachbesserungen in angewendeten Verfahren gravierende Datenschutzverletzungen nicht abgestellt oder verhindert werden können. In diesen Fällen erstreckt sich die Befugnis der Aufsichtsbehörden dann auch darauf, Verarbeitungen zeitweise zu beschränken oder sogar dauerhaft zu verbieten. Ein Verbot der

Datenübermittlung an Drittländer oder internationale Organisationen kann ebenfalls ausgesprochen werden.

Für die Praxis ist nicht anzunehmen, dass es im öffentlichen Umfeld zum Ausspruch von Verarbeitungsverboten für Auftragsverarbeiter kommt, wenn Verarbeitungsvorgänge betroffen sind, welche für die Erfüllung von gesetzlichen Aufgaben zwingend notwendig sind.

Augenmerk verdient Art. 58 Abs. 2 lit. i. Dieser ermächtigt die Aufsichtsbehörde, ein Bußgeld gemäß Art. 83 zu verhängen. Nach § 43 Abs.3 BDSG-Anpassungsgesetz vom 5. Juli 2017 werden „gegen Behörden und sonstige öffentliche Stellen [...] keine Geldbußen verhängt." Aus heutiger Sicht ist nicht erkennbar, dass in den novellierten Landesdatenschutzgesetzen andere Festlegungen getroffen werden. **Somit kann davon ausgegangen werden, dass die Bußgelddrohung aus der DSGVO für öffentliche IT-Dienstleister nicht greift.**

11 Datenschutzbeauftragter

Die DSGVO fordert in Art. 37 Abs. 1 lit. a von öffentlichen IT-Dienstleistern zwingend die Bestellung eines Datenschutzbeauftragten und eines Stellvertreters. Dies gilt gemäß Art. 37 Abs. 1 lit. b DSGVO auch für Dienstleister, die in privater Rechtsform Auftragsdatenverarbeitung für öffentliche verantwortliche Stellen durchführen. In Abhängigkeit von Rechts- und Organisationsform des Auftragsverarbeiters war das nach bisherigem Recht nicht in jedem Fall vorgeschrieben. **Gegebenenfalls sind entsprechende Bestellungen bis spätestens 25. Mai 2018 nachzuholen.** Dabei gilt:

- Die Bestellung erfolgt gemäß Art. 37 Abs. 1 durch „den Auftragsverarbeiter“, also durch die jeweilige Behörden- oder Unternehmensleitung.
- Mehrere Auftragsverarbeiter in der Rechtsform von Behörden oder öffentliche Stellen dürfen gemäß Art. 37 Abs. 3 DSGVO nach dessen Maßgabe einen gemeinsamen Datenschutzbeauftragten bestellen.

Der Datenschutzbeauftragte berichtet unmittelbar der Behördenleitung („höchste Managementebene des Verantwortlichen oder des Auftragsverarbeiters“). Dabei handelt es sich nicht nur um ein Berichtsrecht, sondern um eine Berichtspflicht. Zweckmäßigerweise sollte der Datenschutzbeauftragte dazu organisatorisch in seiner Funktion auch dort angebunden werden. Das sichert zudem seine Unabhängigkeit (Art. 38 Abs. 3 DSGVO), seine Ausstattung mit den zur Erfüllung seiner Aufgaben erforderlichen Ressourcen (Art. 38 Abs. 2 DSGVO) und erleichtert die ordnungsgemäße und frühzeitige Einbindung in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen (Art. 38 Abs. 1 DSGVO).

Insbesondere für kleinere Verwaltungen oder IT-Dienstleister dürfte es von Interesse sein, dass dem Datenschutzbeauftragten neben seinen originären Tätigkeiten auch andere Aufgaben übertragen werden dürfen, soweit dies nicht zu Interessenskonflikten führt (Art. 38 Abs. 6 DSGVO).

Der behördliche Datenschutzbeauftragte erfüllt seine Aufgaben eigenverantwortlich. Er ist dabei unabhängig und weisungsfrei und zur Vertraulichkeit und Geheimhaltung verpflichtet. Aufgrund der Bestimmung in Art. 38 Abs. 5 DSGVO bedarf es im Gegensatz zum bisherigen Recht, das eine Verpflichtung auf das Datengeheimnis vorsah, keiner gesonderten Geheimhaltungsverpflichtung für den Datenschutzbeauftragten mehr. Er darf wegen der Erfüllung seiner Aufgaben weder abberufen noch benachteiligt werden (Art. 38 Abs. 3 DSGVO).

Hinsichtlich der geforderten Qualifikation des Datenschutzbeauftragten folgt aus Art. 37 Abs. 5 DSGVO, dass er über das gebotene Fachwissen auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis verfügt und die Fähigkeit besitzt, die in Art. 39 DSGVO beschriebenen Aufgaben zu erfüllen.

12 Verzeichnis von Verarbeitungstätigkeiten

Nach Art. 30 Abs. 2 DSGVO müssen Auftragsverarbeiter ein „Verzeichnis von Verarbeitungstätigkeiten“ führen. Diese Verpflichtung gab es in dieser Form nach altem Recht nicht. Bisher waren nur die „datenverarbeitenden Stellen“ (jetzt: „Verantwortliche“) gehalten, Verfahrensverzeichnisse zu führen. **Das neue Recht verlangt von den Auftragsverarbeitern, in einem Verzeichnis unter Angabe der eigenen Identifikations- und Kontaktdaten zu dokumentieren, für welche Auftraggeber sie tätig sind, welche Kategorien von Daten für jeden einzelnen Auftraggeber verarbeitet werden, welche Datenübermittlungen an Drittländer zur Erfüllung seiner Aufgaben erfolgen und, „wenn möglich“, in allgemeiner Form zu beschreiben, welche technischen und organisatorischen Maßnahmen zur Sicherheit der Verarbeitung getroffen wurden.** Die Pflicht besteht auch für IT-Dienstleister, die weniger als 250 Mitarbeiter beschäftigen, da sie Aufgrund ihrer Aufgabenstellung nicht nur gelegentlich tätig sind (Art. 30 Abs. 5 DSGVO). Das Verzeichnis ist zudem der zuständigen Aufsichtsbehörde auf Anfrage zur Verfügung zu stellen.

Im Einzelnen muss das Verzeichnis enthalten:

- Namen und Kontaktdaten des Auftragsverarbeiters
- Name und Kontaktdaten seines Datenschutzbeauftragten
- Namen und Kontaktdaten der Verantwortlichen (= Auftraggeber)

- Kategorien von Verarbeitungen, die im Auftrag jedes Verantwortlichen durchgeführt werden
- Übermittlungen personenbezogener Daten an ein Drittland (mit Angabe des Landes) oder eine internationale Organisation (mit deren konkreter Bezeichnung), soweit diese auf Veranlassung des Auftragsverarbeiters erfolgen.
- Wenn möglich eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Art. 32 Abs. 1 DSGVO.

Die Relativierung aus dem letzten Punkt („wenn möglich“) dürfte für professionelle IT-Dienstleister nicht zum Tragen kommen. Sie ist nur für den Fall relevant, dass auch der Auftragsverarbeiter die speziellen Verarbeitungsätigkeiten nicht selbst wahrnimmt, sondern einen weiteren Dienstleister damit beauftragt. Dann müssen sie allerdings in dessen Verzeichnis von Verarbeitungstätigkeiten dokumentiert werden. Die DSGVO macht keine Vorgaben, an welcher Stelle innerhalb der Organisation eines Verantwortlichen das Verfahrensverzeichnis zu führen ist. Einerseits enthält das Verzeichnis eine Auflistung aller relevanten Kunden-/Auftragsbeziehungen, was für eine zentrale Zuordnung, zum Beispiel beim Vertrieb oder Vertragsmanagement spricht, wie sie auch von der Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD) empfohlen wird. Andererseits sind aber auch anwendungs- oder verfahrensspezifische Informationen enthalten, die eine dezentrale Zuordnung sinnvoll erscheinen lassen (soweit ein einheitlicher Aufbau sichergestellt ist). **Die Rechtskonformität ist sicher am besten herzustellen, wenn die Führung des Verfahrensverzeichnisses einer (zentralen) Stelle obliegt, der seitens der Fachabteilungen zugearbeitet werden muss.** Es gibt keinen zwingenden Grund, die Führung des Verfahrensverzeichnisses dem Datenschutzbeauftragten zu übertragen.

13 Weiterführende Informationen

Weiterführende Information, auch zu Fragen der Operationalisierung gibt es auf den Internetpräsenzen von Datenschutzorganisationen, berufsständischen Vereinigungen und Aufsichtsbehörden. Diese Linkliste bietet eine erste Übersicht.

https://www.gdd.de/aktuelles/startseite/noch-100-tage-bis-anwendung-der-ds-gvo/

https://www.bvdnet.de/themen/gdpr/

https://www.datenschutzzentrum.de/dsgvo/

https://www.bfdi.bund.de/DE/Datenschutz/DatenschutzGVO/Aktuelles/Aktuelles_Artikel/DSGVO_Kurzpapiere.html