IHK-AnwenderClub Datenschutz und Informationssicherheit

Praxisleitfaden

Auftragsverarbeitung gemäß Artikel 28 EU-DS-GVO
Anforderung an die betriebliche Organisation

Redaktion: Rudi Kramer | Ulrich Neef - Koordination: Gerd Schmidt | Knut Harmsen

IHK
Industrie- und Handelskammer
Nürnberg für Mittelfranken

Best practice Guide zur EU DS-GVO

Herausgeber
IHK Nürnberg für Mittelfranken
Ulmenstraße 52
90443 Nürnberg
Tel. 0911 1335-335 | Fax -150335
www.ihk-nuernberg.de

Redaktion
Arbeitsgruppe Auftragsverarbeitung des IHK-AnwenderClubs Datenschutz und Informationssicherheit
Redaktionelle Leitung: Rudi Kramer und Ulrich Neef
Koordination: Gerd Schmidt und Knut Harmsen

Kontakt
Industrie- und Handelskammer Nürnberg für Mittelfranken
Geschäftsbereich Innovation und Umwelt
Richard Dürr
Tel. 0911 1335-320
E-Mail: richard.duerr@nuernberg.ihk.de

Bildnachweis Titelseite
Bild: Yakobchuk, iStockphoto.com

Erstveröffentlichung: August 2017
2. Auflage: Februar 2018

Inhaltsverzeichnis

Hinweise
Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung männlicher und weiblicher Sprachformen und Titel verzichtet. Sämtliche Personenbezeichnungen gelten gleichwohl für beiderlei Geschlecht.

Ergänzende Dokumente / Mitgeltende Unterlagen

Kurzbeschreibung	Dokumententitel	Referenz
DS-GVO	VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)	http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679&from=DE
Working Paper der Art. 29-Gruppe WP169	Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter" vom 16.02.2010	http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_de.pdf
Kurzpapier der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz –DSK)	Kurzpapier Nr. 13 Auftragsverarbeitung, Art. 28 DS-GVO	https://www.lda.bayern.de/media/dsk_kpnr_13_auftragsverarbeitung.pdf
OH Cloud-Computing	Orientierungshilfe – Cloud-Computing der Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Arbeitsgruppe Internationaler Datenverkehr des Düsseldorfer Kreises; Stand 09.10.2014	https://www.datenschutz-bayern.de/technik/orient/oh_cloud.pdf
5. TB BayLDA	5. Tätigkeitsbericht des Bayerischen Landesamtes für Datenschutzaufsicht für die Jahre 2011-2012	https://www.lda.bayern.de/media/baylda_report_05.pdf
6. TB BayLDA	6. Tätigkeitsbericht des Bayerischen Landesamtes für Datenschutzaufsicht für die Jahre 2013-2014	https://www.lda.bayern.de/media/baylda_report_06.pdf
Anmerkungen zur Auftragsverarbeitung	Unverbindliche Anmerkungen des Bayerischen Landesamtes für Datenschutzaufsicht vom 26.10.2016	https://www.lda.bayern.de/media/baylda_ds-gvo_10_processor.pdf
Mustervertrag AV Bayerisches Landesamt für Datenschutzaufsicht	Formulierungshilfe für einen Auftragsverarbeitungsvertrag nach Art. 28 Abs. 3 DS-GVO1	https://www.lda.bayern.de/media/muster_adv.pdf
AV-Muster GDD Gesellschaft für Datenschutz und Datensicherheit	Mustervertrag zur Auftragsdatenverarbeitung	https://www.gdd.de/aktuelles/startseite/vertragsmuster-zur-auftragsverarbeitung
Mustervertragsanlage AV BITKOM Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.	Mustervertragsanlage Auftragsverarbeitung i. S. d. Art. 28 Abs. 3 Datenschutz-Grundverordnung (DS-GVO)	https://www.bitkom.org/NP-Themen/NP-Vertrauen-Sicherheit/Datenschutz/EU-DSG/170515-Auftragsverarbeitung-Anlage-Mustervertrag-online.pdf
Erläuternde Hinweise zur AV BITKOM Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.	Begleitende Hinweise zu der Anlage Auftragsverarbeitung; Leitfaden	https://www.bitkom.org/NP-Themen/NP-Vertrauen-Sicherheit/Datenschutz/EU-DSG/170515-LF-Auftragsverarbeitung-online.pdf

Für die Richtigkeit der Links bzw. bezüglich der Inhalte der verlinkten Dokumente wird keine Gewähr übernommen.

Information zur Arbeitsgruppe

Wir danken folgenden Personen für die Mitwirkung an diesem Praxisleitfaden:

Name	**Firma**
Dr. Lutz-Steffen Berghold	Eckart GmbH
Walter Biller	Biller Dienstleistungen
Jens Hansen	Maschinenfabrik Niehoff GmbH & Co. KG
Knut Harmsen	IHK Nürnberg für Mittelfranken
Antje Herrmann	uniVersa Lebensversicherungs a.G.
Rudi Kramer	DATEV eG
Ulrich Neef	SoftKom e.K.
Christian Regnet	BNP Paribas S.A. NL Deutschland
Reiner Schmalzl	Telekom Deutschland
Jürgen Schmidt	BUSCON Business- & IT-Consulting
Rigobert Uhe	Siemens AG

Einleitung

Kaum ein Unternehmen kann alle personenbezogenen Daten, die im Rahmen seiner Geschäftstätigkeit verarbeitet werden, ohne die Hinzuziehung eines Dienstleisters verarbeiten: Sei es die Einschaltung eines Callcenters bei der Kundenbetreuung, der Erwerb von Daten zur Bewerbung neuer Kunden, der Zugriff auf personenbezogene Daten im Supportfall hinsichtlich der eigenen IT durch einen externen Experten, die Auslagerung von Daten in eine internetbasierte Lösung („Cloud"), die Beauftragung eines Rechtsanwalts oder Steuerberaters, denen zur Beratung auch personenbezogene Daten weitergegeben werden müssen, bis hin zur Regelung der Entsorgung von Akten und Festplatten durch einen Spezialisten: in all diesen Fällen ist die datenschutzrechtliche Behandlung zu prüfen und zu regeln. Bislang galt hier das BDSG (Bundesdatenschutzgesetz), welches zum 25.05.2018 durch die Datenschutz-Grundverordnung (DS-GVO) abgelöst wird. Zwar hat der Gesetzgeber bereits ein BDSG-neu beschlossen, welches ebenfalls ab 25.5.2018 gelten wird. Die dortige Regelung zur Auftragsverarbeitung in § 62 betrifft aber ausschließlich die Datenverarbeitung im Auftrag für Behörden auf Bundesebene im Rahmen der Strafverfolgung und wird für die meisten Unternehmen nicht anwendbar sein.

Die fristgerechte Umstellung auf die künftige Rechtslage der DS-GVO und somit zu rechtskonformen Verhalten liegt im ureigensten Interesse einer jeden Unternehmensleitung, für viele vor allem wegen der drastisch erhöhten Sanktionen. Selbst wenn ein interner oder externer Datenschutzbeauftragter das Unternehmen berät: Verantwortlich für die Einhaltung der gesetzlichen Vorschriften ist das Management des Unternehmens. An dieses richtet sich dieser Leitfaden. Die Auftragsverarbeitung ist ein wesentlicher Bestandteil des Datenschutzmanagements und der Art. 28 DS-GVO wird zu einer zentralen Norm in der Umsetzung der DS-GVO. Auch wenn zum Zeitpunkt des redaktionellen Abschlusses weiterhin noch Detailfragen hinsichtlich Auslegung und Subsumtion offen und in der europäischen Meinungsbildung noch zu klären sind, versucht der Leitfaden auf Thematiken aufmerksam zu machen, Lösungswege zu skizzieren und Hilfestellungen zu geben. Die Verfasser bemühten sich praxisnahe Herangehensweisen zu schildern und hoffen auf regen Gebrauch und Nutzen für die Leser. Für die behördliche Prüfpraxis wird von Interesse sein, dass mit der Einholung Nachträgen zur bestehenden Auftragsdatenvereinbarungen bereits geraume Zeit vor Geltung der DS-GVO begonnen wurde und ein Prozess zur Einholung entsprechender Nachträge aufgesetzt wurde. Bei Einhaltung dieser Vorgaben dürfte nicht erwartet werden, dass bis zum 25.05.2018 alle Nachträge eingeholt sind, gerade wenn eine Vielzahl von Vereinbarungen anzupassen sind.

Koordination: Gerd Schmidt und Knut Harmsen

1. Grundsätze der Auftragsverarbeitung

1.1 Einführung

In der DS-GVO ändert sich an den Grundsätzen bei der Auftragsverarbeitung wenig: Der Auftraggeber bleibt als Verantwortlicher für die Einhaltung der Rechtmäßigkeitsanforderungen und Betroffenenrechte weiterhin in der Pflicht. Konkretisiert werden nun auch auf europäischer Ebene die Regelungsinhalte einer Vereinbarung zur Auftragsverarbeitung, was wir aus dem BDSG bereits seit der BDSG-Novellierung in 2009 kennen. **Gestiegen sind die Anforderungen an den Auftragsverarbeiter**, der nun stärker in die Pflicht genommen wird, sei es bei den Dokumentationspflichten wie dem Führen eines Verzeichnisses der Verarbeitungstätigkeiten nach Art. 30 Abs. 2 oder der direkten Adressierung der Vorschriften zur Sicherheit der Verarbeitung in Art. 32. Auch die Einbindung eines Subunternehmers wird formalisierter gestaltet.

Inwieweit bisherige Festlegungen und rechtliche Zuordnungen, die die Aufsichtsbehörden und auch die Art.-29-Datenschutzgruppe (die Arbeitsgemeinschaft der Europäischen Datenschutzaufsichtsbehörden) getroffen haben, bestehen bleiben können, ist abzuwarten. Da sich die Definitionen des Verantwortlichen und des Auftragsverarbeiters aus der Richtlinie 95/46/EG (die den Datenschutz bislang auf europäischer Ebene vorgab) und der DS-GVO im Wesentlichen nicht unterscheiden, kann unterstellt werden, dass die Ausführungen aus dem Working Paper 169 der Art.-29-Gruppe weiterhin gelten.

Änderungen ergeben sich bei der Inanspruchnahme fremder Leistungen bei einem Verantwortlichen, für die bei der Verarbeitung (einschließlich Übermittlung) personenbezogener Daten eine Rechtsgrundlage gemäß Art. 6 DS-GVO bzw. nach Art. 9 und Art. 6 DS-GVO (kumulative Anwendung von Art. 9 und Art. 6 DS-GVO) bei Verarbeitung von besonderen Kategorien personenbezogener Daten gegeben sein muss. Hier wurde bislang von einer „**Funktionsübertragung**" gesprochen. Damit wurde die Beauftragung eines Dienstleisters bezeichnet, der dann aber eine neue verantwortliche Stelle ist. Der Begriff stammt aus einer Gesetzesbegründung des BDSG in Abgrenzung zu einer technischen Hilfeleistung eines Dienstleisters. Bei der Funktionsübertragung übernimmt der Dienstleister eine eigene Verantwortlichkeit für die Aufgabe, für die Weitergabe der personenbezogenen Daten ist eine eigene Rechtmäßigkeitsgrundlage erforderlich.[1] Diese Tätigkeiten werden durch die Datenschutzkonferenz, einer Arbeitsgemeinschaft der deutschen Aufsichtsbehörden, nun unter Aufgabe des Begriffs der Funktionsübertragung (weiterhin) nicht als Auftragsverarbeitung klassifiziert. Dies betrifft beispielsweise die Einbeziehung eines Berufsgeheimnisträgers (Steuerberater, Rechtsanwälte, externe Betriebsärzte, Wirtschaftsprüfer), Inkassobüros mit Forderungsübertragung, Bankinstituts für den Geldtransfer und Postdienstes für den Brieftransport.[2]

Eine weitere Abgrenzung kann sich zu Art. 26 ergeben, der **„**gemeinsamen Verantwortlichkeit**"** für eine Verarbeitung. Dabei legen zwei Verantwortliche gemeinsam Zwecke und Mittel einer Verarbeitung fest. Der Gesetzgeber fordert dazu, dass sie in transparenter Form festlegen, wer von ihnen welche Verpflichtungen gemäß dieser Verordnung erfüllt. Die Datenschutzkonferenz zählt hierzu beispielsweise klinische Arzneimittelstudien, wenn mehrere Mitwirkende (z. B. Sponsoren, Studienzentren/ Ärzte) jeweils in Teilbereichen Entscheidungen über die Verarbeitung treffen oder die gemeinsame Verwaltung bestimmter Datenkategorien (z.B. „Stammdaten") für bestimmte gleichlaufende Geschäftszwecke mehrerer Konzernunternehmen.[3]

[1] 5. Tätigkeitsbericht des BayLDA, Ziffer 5.1
[2] Datenschutzkonferenz, 13. Kurzpapier zur Auftragsverarbeitung, Anhang B , Stand 16.01.2018
[3] Datenschutzkonferenz-Kurzpapier Nr. 13 zur Auftragsverarbeitung, Anhang C, Stand 16.01.2018

Es ist davon auszugehen, dass sich auch in der europäischen Auslegung der DS-GVO daran nichts ändert, da auch die Art. 29 Datenschutzgruppe im Working Paper 169 zu der Thematik Verantwortlicher und Auftragsverarbeiter aus dem Jahr 2010 hierzu Beispielsfälle nannte. Unabhängig davon ob die Begrifflichkeit („Funktionsübertragung") verwendet oder sich eine neue auf europäischer Ebene bilden wird, es wird sich voraussichtlich in bestimmten Situationen wie beispielsweise bei medizinischen Gutachten, Rechts- und Steuerberatung die datenschutzrechtliche Einordnung nichts ändern. Als Auftraggeber genüge es dabei, dass allgemeinere Regelungen zu den durchzuführenden Tätigkeiten, zur Zweckbindung von übermittelten Daten und zur Geheimhaltung getroffen würden, weil die dort geltenden berufsrechtlichen Vorschriften (Steuerberatungsgesetz, Ärztliche Berufsordnungen, § 203 Abs. 1 StGB, usw.) schon Grenzen ziehen und eigenverantwortliche Pflichten auch zur Verschwiegenheit und Vertraulichkeit festlegen. Zudem besteht dort auch noch eine berufsrechtliche Kammeraufsicht, die für die Einhaltung der rechtlichen Pflichten ihrer Kammer- Mitglieder zuständig ist.[4]

Auftragsverarbeitung liegt auch beim sogenannten **Cloud-Computing** vor, hier bietet der Dienstleister eine in der Regel skalierbare Leistung (Datenverarbeitung) über das Internet an. Auch allein die Speicherung zählt zu den Verarbeitungstätigkeiten. Inwieweit Aussagen aus der Orientierungshilfe Cloud-Computing der Deutschen Aufsichtsbehörden auch unter der DS-GVO anzuwenden sein werden, wird sich zeigen, dies betrifft beispielsweise die Forderung, dass ein Auftraggeber nicht auf ein Überprüfungsrecht vor Ort vertraglich verzichten darf. Nach Ansicht des Bayerischen Landesamtes für Datenschutzaufsicht (BayLDA) liegt keine Auftragsverarbeitung vor, wenn die Daten beim Dienstleister mit einer aktuellen Verschlüsselungstechnologie vor einer möglichen Kenntnisnahme durch den Dienstleister geschützt sind.[5]

Die Datenschutzkonferenz hat sich zu der Frage der Beurteilung bei Wartungstätigkeiten positioniert. Sachverhalte, die bislang unter § 11 Abs. 5 BDSG fielen, und danach in entsprechender Weise als Auftragsverarbeitung zu behandeln waren, sollen nun direkt als Auftragsverarbeitung behandelt werden.[6] Demnach müssten bei **Wartungs- und Prüfungstätigkeiten** von Datenverarbeitungsanlagen, bei denen der Dienstleister personenbezogene Daten zur Kenntnis nehmen könnte, die Vorgaben zur Auftragsverarbeitung erfüllt werden. Eine explizite Regelung gibt es in der DS-GVO dazu nicht. Die derzeitigen Einschätzungen der deutschen Aufsichtsbehörden sind auf europäischer Ebene durch die Art. 29 Datenschutzgruppe noch nicht bestätigt.

Auch ist davon auszugehen, dass ein Sachverhalt nicht als Auftragsverarbeitung bewertet wird, wenn die Möglichkeit einer Kenntnisnahme durch den Dienstleister nicht durch Einrichtungen der EDV erfolgt, beispielsweise bei mechanischen Reparaturen von datenverarbeitenden Anlagen beim Auftraggeber. Bei anderen Sachverhalten wie der Fernwartung ist in der Diskussion, inwieweit hier eine Verarbeitung vorliegt: Der Auftrag an den Dienstleister umfasst in diesen Fällen nicht die Verarbeitung der personenbezogenen Daten im engeren Sinne, sondern die Fehleranalyse bzw. Fehlerbeseitigung. Folgt man der Ansicht der Datenschutzkonferenz und erweitert die Auftragsverarbeitung auf die Möglichkeit einer Kenntnisnahme durch den System wartenden Dienstleister, gibt es aber keine praktikable Lösung, wie die daraus entstehenden Anforderungen hinsichtlich Subunternehmer (weiterer Auftragsverarbeiter iSd Art. 28 Abs. 2 DS-GVO) zu gestalten sind.
Letztendlich wird man bei dieser Thematik die Meinungsbildung auf europäischer Ebene abwarten müssen, wozu unter Umständen nicht nur die Art. 29 Datenschutzgruppe, sondern auch der Europäische Gerichtshof beitragen werden.

[4] 6. Tätigkeitsbericht des BayLDA, Ziffer 5.6
[5] 6. Tätigkeitsbericht des BayLDA Ziffer 5.2
[6] Datenschutzkonferenz-Kurzpapier Nr. 13 zur Auftragsverarbeitung, Seite 3, Stand 16.01.2018

Die Regelungen zur Auftragsverarbeitung sind allerdings dann nicht anwendbar, wenn der Dienstleister bei der Wartung nur Daten zur Kenntnis nehmen kann, die er selbst nicht oder nur mit großem Aufwand einer natürlichen Person zuordnen kann. So ist beispielsweise eine Emailadresse „service@Unternehmen.de" für den Dienstleister nicht ohne Weiteres personenbeziehbar, solange er nicht weiß, bzw. nur mit einem großen Aufwand herausfinden könnte, welche Beschäftigten beim Auftraggeber dieser Funktionsemailadresse tatsächlich zugeordnet sind. Wird ihm mit der Beauftragung auch noch vertraglich untersagt, einen Personenbezug zu dieser Funktionsemailadresse herzustellen, so ist davon auszugehen, dass hierfür die Regelungen der Auftragsverarbeitung nicht erforderlich sind.
Näheres zur Einbindung von Subunternehmern siehe unter Ziffer 2.

1.2 Handlungsfelder

- Prüfen Sie Ihre bestehenden Vereinbarungen zur Auftragsdatenverarbeitung.
- Überprüfen Sie Ihre bestehenden vertraglichen Gestaltungen im Hinblick auf ein Delta zu den inhaltlichen Anforderungen der DS-GVO und passen Sie bestehende Verträge (die über den 25.05.2018 hinaus gelten) per Nachtrag entsprechend an.[7]
- Eruieren Sie, bei welchen Auftragsverarbeitungen ein Subunternehmer (weiterer Auftragsverarbeiter) eingesetzt wird und welchen Leistungsteil er übernimmt.
- Führen Sie gemeinsam mit Ihren rechtlichen Experten, wie Rechtsabteilung oder externe Kanzlei, eine Entscheidung herbei, ob die bestehende vertragliche Gestaltung per Nachtrag zu ergänzen oder neu abzuschließen ist.
- Entscheiden Sie, ob Sie Schriftformerfordernis oder die dokumentierte Textform fordern.
- Entscheiden Sie, ob Sie auch Musternachträge Ihrer Dienstleister zur Auftragsdatenverarbeitung akzeptieren (ggf. hoher Prüfaufwand durch den Bereich Datenschutz) oder ausschließlich ein eigenes Muster an Auftragsverarbeiter herausgeben wollen.
- Setzen Sie möglichst frühzeitig einen Prozess zur Einholung der Nachträge zur Vereinbarung zur Auftragsverarbeitungauf und binden Sie Ihren Einkauf bzw. die zuständigen Produktverantwortlichen ein.
- Prüfen Sie mit Ihrem Einkauf, und den sonstigen betroffenen (Abteilungen), die Dienstleister anbinden, ob Sie für jeden Dienstleister, der personenbezogene Daten für Sie verarbeitet, eine Vereinbarung zur Auftragsverarbeitung abgeschlossen haben und Ihren Nachweispflichten nachkommen können.
- Bis dato etwaige fehlende Auftragsdatenvereinbarungen sind durch Auftragsverarbeitungsvereinbarungen nach DS-GVO nachzuziehen. Beachten Sie hierzu die folgenden Kapitel.
- Stellen Sie im Rahmen Ihres Datenschutzmanagements eine (zentrale) Archivierung der Auftragsdatenvereinbarungen, der Nachträge sowie der zukünftig neu abzuschließenden Verträge sicher, um jederzeit kurzfristig der Rechenschaftspflicht nachkommen zu können.

1.3 Sanktionen

In Art. 83 Abs. 4 lit. a) werden Verstöße gegen die Vorgaben zur Auftragsverarbeitung mit Geldbuße bis 10 Mio. Euro oder 2 % des weltweiten Jahresumsatzes geahndet, je nachdem welcher der Beträge höher ist.
Dies kann auch den Auftragsverarbeiter treffen!

[7] Die GDD hat beispielsweise eine Synopse zu ihrem bisherigen Mustervertrag erstellt

2. Subunternehmen

2.1 Einführung

Die Einbeziehung von weiteren Auftragsverarbeitern (Subunternehmern) wird formalisierter. Verlangte § 11 Abs.2 BDSG bisher nur, dass eine Regelung hierzu getroffen wird, fordert die DS-GVO, dass der Verantwortliche als Auftraggeber jedem Subunternehmer vorher schriftlich zustimmt. In der veröffentlichten Formulierungshilfe zur Auftragsverarbeitung des BayLDA, heißt es, dass eine Zustimmung nur erteilt werden kann, wenn der Auftragnehmer dem Auftraggeber Namen und Anschrift sowie die vorgesehene Tätigkeit des Subunternehmers mitteilt. Die Anforderung an die Schriftlichkeit wird sich über den Verweis auf Art. 28 Abs. 9 sicher auch als elektronische Zustimmung auslegen lassen. Empfehlenswert ist es aber, künftig klar zu definieren, wer im Kontext des Vertrages als weiterer Auftragsverarbeiter (Subunternehmertätigkeit) zu betrachten ist. Die bisherigen Vertragsmuster der GDD oder des BITKOM hatten auch bislang schon eine Abgrenzung vorgesehen.[8] Eine Möglichkeit wäre, die zu genehmigenden Subunternehmertätigkeiten auf die Durchführung der im Vertrag vereinbarten Leistungen zu definieren. Beispielsweise wäre dies bei einem Callcenter, wenn ein weiteres Callcenter mit der Durchführung einer Teil- oder der gesamten vereinbarten Leistung durch den Dienstleister beauftragt würde. Noch nicht abschließend geklärt ist auf europäischer Ebene, ob auch der Wartungspartner des Callcenters oder des Sub-Callcenters der die Telefonanlage betreut ebenfalls als weiterer Auftragsverarbeiter aus Sicht des Hauptauftraggebers und des Verantwortlichen zu definieren ist.

Sollte man sich für eine Bewertung von diesen Wartungstätigkeiten als Auftragsverarbeitung entscheiden, ist auch eine Regelung über die Zustimmung beim Wechsel der Wartungsdienstleiter zu vereinbaren. Insbesondere bei standardisierten Dienstleistungen, die einer Vielzahl von Auftraggebern angeboten werden, kann sich hier ein Problem in der Praxis bilden, wenn jeder einzelne Auftraggeber zustimmen muss.

2.2 Erwägungsgründe zu Subunternehmer

In den Erwägungsgründen 81 und 101 finden sich Ausführungen, die zur Auslegung herangezogen werden können, insb. zu den Anforderungen bei der Auswahl des Dienstleisters und der Festlegung, dass die Auftragsverarbeitung auch außerhalb der Europäischen Union bzw. des Europäischen Wirtschaftsraums erfolgen kann.

2.3 Referenzierende Artikel zu Subunternehmen

Regelungen zu weiteren Auftragsverarbeitern finden sich in Art. 28 Abs. 2 und Abs. 4 DS-GVO.

2.4 Handlungsfelder zu Subunternehmer

- Definieren Sie für sich, was Sie unter Subunternehmer (weitere Auftragsverarbeiter) verstehen und klären Sie dieses Verständnis mit Ihrem Dienstleister / Auftraggeber.
- Bestimmen Sie genau die vorgesehene oder derzeitige Tätigkeit ihrer Subunternehmer. Zu empfehlen ist, jeden einzelnen eingesetzten Subunternehmer namentlich mit Firmierung, Anschrift und übernommener Tätigkeit/Datenverarbeitung zu benennen.

[8] GDD Mustervertrag; bitkom Mustervertragsanlage zur DS-GVO

- Informieren Sie den Einkauf / Ihre Produktverantwortlichen, damit diese prüfen können, wo bislang Subunternehmerverhältnisse existieren, die als weitere Auftragsverarbeiter zu bewerten sind.
- Gehen Sie in die Verhandlungen mit den Dienstleistern / Auftraggebern, um ein gemeinsames Verständnis zu erreichen.
- Werden Auftragsverarbeitungen durch den Dienstleister im außereuropäischen Ausland erbracht, beachten Sie das Kapitel 5 „Drittstaaten".
- Relevant sind nur die Auftragsverhältnisse, bei denen Leistungen auch nach dem 25.05.2018 erbracht werden.

2.5 Sanktionen

In Art. 83 Abs. 4 lit. a) werden Verstöße gegen die Vorgaben zur Auftragsverarbeitung mit Geldbuße bis 10 Mio. Euro oder 2 % des weltweiten Jahresumsatzes geahndet, je nachdem welcher der Beträge höher ist.
Dies kann auch den Auftragsverarbeiter treffen!

3. Vertragliche Anforderungen

3.1 Vertragliche Anforderungen

Gemäß Artikel 28 Abs. 3 hat die Verarbeitung durch einen Auftragsverarbeiter auf der Grundlage eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht der Mitgliedstaaten zu erfolgen. Die Parteien können entscheiden, ob sie einen individuellen Vertrag oder Standardvertragsklauseln verwenden. Der Vertrag kann schriftlich oder in elektronischer Form abgeschlossen werden. Dies bedeutet, dass auch online eine Vereinbarung zur Auftragsverarbeitung abgeschlossen werden kann. Hierbei ist zu beachten, dass beide Seiten ihrer Dokumentations-und Nachweispflicht nachkommen können.

Den vertraglichen Anforderungen an eine Vereinbarung zur Auftragsverarbeitung kommt entscheidende Bedeutung zu.

Im Folgenden sollen daher die Erwägungsgründe, referenzierenden Artikel, Handlungsfelder, Checklisten, Kontrollen und Sanktionen aufgeführt und erläutert werden sollen.

3.2 Erwägungsgründe zu vertraglichen Anforderungen

In den Erwägungsgründen 81 und 95 finden sich Ausführungen, die zur Auslegung herangezogen werden können.

3.3 Referenzierende Artikel zu vertraglichen Anforderungen

Regelungen zu den vertraglichen Anforderungen finden sich in Art. 28 Abs. 3 und Abs. 4 und Art. 44 DS-GVO.

3.4 Handlungsfelder zu vertraglichen Anforderungen

1. Implementierung eines unternehmensinternen Prozesses, als ein Baustein des Datenschutzmanagementsystems, der sicherstellt, dass mit allen Dienstleistern, die als Auftragsverarbeiter tätig werden, eine entsprechende vertragliche Grundlage (einschließlich technischer

und organisatorischer Maßnahmen etc.) geschaffen ist, um der Rechenschaftspflicht Genüge tun zu können. Der Prozess sollte beinhalten, dass der Datenschutzbeauftragte bei externer Auftragsvergabe, bei der personenbezogene Daten verarbeitet werden, eingebunden wird, um sicherstellen zu können, dass Auftragsvereinbarungen mit den erforderlichen Regelungen geschlossen werden. Im Vorfeld des Vertragsabschlusses ist durch den Verantwortlichen sicherzustellen, dass nur Dienstleister ausgewählt werden, die für die konkrete Datenverarbeitung risikobasierte technische und organisatorische Maßnahmen getroffen haben, welche die Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten entsprechend berücksichtigen und den Risiken wirksam begegnen und eine Datenverarbeitung im Einklang mit der DSGVO garantieren.

2. Aufnahme folgender Regelungen in den Vertrag, dass:

   a. der Auftragsverarbeiter alle gem. Art. 32 erforderlichen Maßnahmen zur Sicherheit der Verarbeitung ergreift;
   b. Subunternehmer (weitere Auftragsverarbeiter) nur nach vorheriger schriftlicher Genehmigung (auch in einem elektronischen Format[9]) beauftragt werden dürfen;
   c. der Auftragsverarbeiter im Falle einer allgemeinen schriftlichen Genehmigung den Verantwortlichen über jede beabsichtigte Änderung bei Subunternehmern informiert;
   d. Subunternehmer (weitere Auftragsverarbeiter) ebenso vertraglich zu verpflichten sind wie der Auftragsverarbeiter, Art. 28 (4);
   e. der Auftragsverarbeiter verpflichtet ist, den Verantwortlichen dabei zu unterstützen, den Anträgen betroffener Personen auf Wahrnehmung ihrer Rechte nach Kapitel III nachzukommen, soweit der Verantwortliche dies nicht selbst vornehmen kann;
   f. sich der Auftragsverarbeiter verpflichtet, den Verantwortlichen bei der Einhaltung der in den Art. 32-36 genannten Pflichten zu unterstützen, soweit der Verantwortliche dies nicht selbst vornehmen kann;
   g. nach Abschluss der Erbringung der (jeweiligen) Vertragsleistungen alle personenbezogenen Daten zu löschen, zu vernichten (sonstige Datenträger) oder zurückzugeben sind. Hinweis: Auch Regelungen zur Vernichtung von Papierunterlagen und von sonstigen Datenträgern aufnehmen. Ausnahme: Verpflichtung zur Speicherung nach Unionsrecht oder dem Recht der Mitgliedsstaaten (z.B. gesetzliche Aufbewahrungspflichten);
   h. der Auftragsverarbeiter dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 32 niedergelegten Pflichten zur Verfügung stellt und Überprüfungen durch den Verantwortlichen ermöglicht werden;
   i. der Auftragsverarbeiter den Verantwortlichen unverzüglich informiert, falls er der Auffassung ist, dass eine Weisung gegen diese Verordnung oder andere Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstößt.
   j. Ggf. außerordentliches Kündigungsrecht und Vertragsstrafe bei schuldhaften Verstößen gegen die Auftragsverarbeitungsvereinbarung, Weisungen, Meldepflichten etc. vereinbaren.

Bei diesen Regelungen, insbesondere zu den Punkten a), a), und a) empfiehlt es sich, bei den vertraglichen Regelungen zu klären, inwieweit hier Leistungen des Auftragnehmers zu einer Änderung der Vergütung führen.

3. Prüfen Sie jeweils, ob für die Auftragsverarbeitung ein individueller Vertrag oder Standard- oder Mustervertragsklauseln gewählt werden sollen[10].

[9] Werden Genehmigungen z.B. per E-Mail erteilt, sollte diese, aufgrund der Anfechtbarkeit, mit einer qualifizierten elektronischen Signatur versehen sein.

[10] Bislang gibt es Musterformulierungen des bitkom und der GDD

4. Sehen Sie im Vertrag dokumentierte Weisungen zur Verarbeitung vor, insbesondere bei Übermittlung in ein Drittland. Diese Weisungen können auch in Leistungsbeschreibungen der vereinbarten Leistung abgebildet werden, wenn diese einbezogen werden.

5. Nehmen Sie eine Regelung zur Vertraulichkeitsverpflichtung betreffend die zur Datenverarbeitung befugten Personen im Vertrag auf, insbesondere, wenn Ihr Unternehmen der Schweigepflicht unterliegt

6. Es ist durch den Verantwortlichen sicherzustellen, dass die Auftragsvereinbarungen (Verträge) mit Auftragsverarbeitern auch bzgl. der Haftungsregelungen Art. 82 EU-DS-GVO entsprechen, d.h., Verantwortlichkeiten und Haftungsregelungen sind aufzunehmen**.** Haftungsregelungen können aber auch im Hauptvertrag (Leistungsvertrag) abgebildet werden.

   Auftragsverarbeiter müssen geeignete und wirksame Maßnahmen so durchführen, dass die Verarbeitung im Einklang mit der Verordnung steht. Bei den zu treffenden Maßnahmen sind die Art der Daten, der Umfang, die Umstände, die Verarbeitungszwecke und das Risiko der Verarbeitung für die Rechte und Freiheiten natürlicher Personen zu berücksichtigen. Dies ist in den Vertrag aufzunehmen und bei der Auswahl des Auftragsverarbeiters im Vorfeld zu berücksichtigen und zu prüfen. Der Verantwortliche muss hierzu im Vorfeld entsprechend der Art der Daten, des Umfangs, der Umstände der Verarbeitung und der Verarbeitungszwecke sowie des Risikos für die Rechte und Freiheiten natürlicher Personen dem Auftragsverarbeiter Vorgaben machen, welche Maßnahmen je nach Risiken zu treffen sind (je nach Risiko vorab auch Datenschutz-Folgenabschätzung durch den Verantwortlichen), prüfen, ob der Auftragsverarbeiter hierzu geeignete Maßnahmen trifft und diese bei der Auswahl berücksichtigen (z.B. Zertifikate vorlegen lassen).

7. Bestandsverträge sind per Nachtrag anzupassen. Dazu ist zu erheben, ob mit allen Auftragsverarbeitern bereits Vereinbarungen zur Auftragsverarbeitung geschlossen sind. Etwaige fehlende Auftragsdatenvereinbarungen sind durch Auftragsverarbeitungsvereinbarungen nachzuziehen und den Abteilungen hierfür ein entsprechendes Muster zur Verfügung zu stellen. Beachten Sie dabei entsprechende zeitliche Vorläufe. Den Abteilungen sind entsprechende Nachträge zu Bestandverträgen als Muster zur Verhandlung mit den Auftragsverarbeitern vorzugeben.

8. Um möglichst im Vorfeld auszuschließen, dass es zum Schadenersatzanspruch kommt, sollten die Abteilungen angewiesen werden, Auftragsverarbeiter sorgfältig auszuwählen, insbesondere sich auch aktuelle Zertifikate etc. vorlegen lassen. Der Auftragsverarbeiter muss das erforderliche Fachwissen für die Durchführung der Auftragsverarbeitung haben.

9. Haftpflichtversicherung:

   a. Auftragsverarbeiter sollten für etwaige Schadenersatzansprüche eine Haftpflichtversicherung abgeschlossen haben, deren Aufrechterhaltung für die gesamte Vertragslaufzeit zu gewährleisten ist. Die Deckungssummen sollten ausreichend sein.
   b. Im Zweifel kann man sich eine Bestätigung der Versicherung bzw. den Versicherungsschein vorlegen lassen.
   c. Entsprechende Regelungen können in der Auftragsvereinbarung getroffen werden.

10. Erweiterte Dokumentationspflicht

    Aufgrund der Rechenschaftspflicht steigt die Anforderung, die vertragliche Vereinbarung ebenso wie Weisungen zu dokumentieren. Die Verträge bzw. Dokumentationen sind zu archivieren. Dies kann auch die Dokumentation über die Regelungen zur Wahrung der Betroffenenrechte, bei denen der Auftragsverarbeiter unterstützen muss, betreffen.

3.5 Sanktionen

In Art. 83 Abs. 4 lit. a) werden Verstöße gegen die Vorgaben zur Auftragsverarbeitung mit Geldbuße bis 10 Mio. Euro oder 2 % des weltweiten Jahresumsatzes geahndet, je nachdem welcher der Beträge höher ist.
Dies kann auch den Auftragsverarbeiter treffen!

3.6 Kontrolle

- Dokumentieren Sie die Prüfung der Archivierung der Vertragsunterlagen
- Überprüfen Sie in regelmäßigen Abständen, insbesondere bei Dauerschuldverhältnissen, ob die gelebte Praxis noch den vertraglichen Regelungen entspricht.

4. Garantien

4.1 Einführung

Aufgrund der hohen Bußgelder für Datenschutzverletzungen muss der Auftragsverarbeiter dem Verantwortlichen hinreichende Garantien für eine datenschutzkonforme Auftragsverarbeitung anbieten. Zertifizierungen spielen dabei eine immer größere Rolle und sind für lukrative Aufträge nicht mehr wegzudenken. Es entsteht auf Grundlage der DS-GVO die Frage, welche Form von Zertifizierungen als eine geeignete Garantie für ein durchgängiges Datenschutzniveau zwischen dem Verantwortlichen und Auftragsverarbeiter angesehen werden kann. Außerdem entsteht die Frage, wie die Einhaltung der Vorschriften zur Auftragsverarbeitung kontrolliert und laufend verbessert werden kann.

Allerdings werden gerade zu Beginn der Anwendung der DS-GVO noch keine Zertifikate oder genehmigte Verhaltensregeln vorliegen. Der Auftraggeber kann daher zunächst auf die Prozessdarstellungen des Auftragnehmers zurückgreifen. Daraus muss ersichtlich sein, dass dieser technische und organisatorische Maßnahmen zur Sicherheit der Verarbeitung vorhält, die auf eine Risikoreduzierung im Hinblick auf die Rechte und Freiheiten der betroffenen Personen zielen.

Das BayLDA sieht zwar keine gesetzliche Verpflichtung für die Schaffung von Datenschutz-Management-Prozessen, jedoch sieht die Behörde die *„… Schaffung eines Datenschutz-Management-Prozesses als erforderlich an, egal wie man es nennt!"*

4.2 Erwägungsgründe zu Garantien

In den Erwägungsgründen 39, Satz 12 und 74 finden sich Ausführungen, die zur Auslegung herangezogen werden können.

4.3 Referenzierende Artikel zu Garantien

Regelungen zu den erforderlichen Garantien finden sich in Art. 5 Abs. 1 lit. f und Abs. 2, sowie Art. 32 Abs. 1 DS-GVO.

4.4 Handlungsfelder

Betreibt der Verantwortliche und/oder der Auftragsverarbeiter ein Managementsystem, bspw. auf Grundlage der ISO/IEC 27001:2013, entstehen für alle Parteien zusätzliche Handlungsfelder, um ausreichende Garantien für eine gesetzeskonforme Auftragsverarbeitung zu gewährleisten. Abgeleitet aus den spezifischen Anforderungen der Norm bieten sich folgende Handlungsfelder an:

- Alle gesetzlichen, regulatorischen, selbstauferlegten oder vertraglichen Anforderungen zum Schutz personenbezogener Daten müssen regelmäßig überprüft werden (Compliance).
- In das Informationssicherheitsmanagement sind die Belange der Auftragsverarbeitung als unterstützender Prozess zu integrieren.
- Adaption der Datenschutzprozesse in das vorhandene Informationssicherheitsmanagement.

Durch die Nachweispflicht des Auftragsverarbeiters zur Eignung bzw. Wirksamkeit von technischen und organisatorischen Maßnahmen können bestehende etablierte Verfahren / Garantien zur Auftragsverarbeitung für Verantwortliche, Auftragsverarbeiter und deren Subunternehmen sein.

Es empfiehlt sich, die Orientierung an genehmigten Verhaltensregeln und Zertifizierungen auszurichten, da diese deutliche Vorteile hinsichtlich der Wirtschaftlichkeit/Kostenreduktion bieten (siehe auch Erwägungsgrund 98).

4.5 Sanktionen

Soweit im Hauptvertrag vereinbart, können Vertragsstrafen (Pönalen) wegen Nichterfüllung oder Untererfüllung von vereinbarten Datenschutzmanagementzielen zwischen Verantwortlichen und Auftragsverarbeitern/Subunternehmern entstehen (Verletzung vereinbarter Maßnahmen). Bei der Verwendung von Klauseln zu Vertragsstrafen empfiehlt es sich qualifizierte fachliche Beratung in Anspruch zu nehmen.

4.6 Kontrolle

- Bestimmen von Schutzzielen[11] hinsichtlich des Verarbeitungsrisikos für die Rechte und Freiheiten natürlicher Personen durch die konkrete Verarbeitung
- Regelmäßige Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung. (Bewertung, ob durch geeignete Maßnahmen das Schutzziel für eine Verarbeitung durch ein Bündel von technischen und organisatorischen Maßnahmen erreicht wurde.)
- Regelmäßige interne Arbeitszirkel der Rollenverantwortlichen bzw. „Asset-Owner"
- Regelmäßiges, vergleichbares Berichtswesen zur Erfolgsmessung von vereinbarten, oder selbstauferlegten Garantien zur sicheren Auftragsverarbeitung

[11] Beispiel: Soll-Vorgaben für die [Daten] - Informationssicherheit personenbezogener Daten unter Berücksichtigung relevanter Gesetze und Vorschriften

5. Drittstaateneinbezug

5. 1 Einführung

Die DS-GVO regelt den Schutz natürlicher Personen bei der Verarbeitung ihrer Daten. Sie hat aber auch das Ziel, den freien Datenverkehr zu ermöglichen. Bei einer Verarbeitung außerhalb der Europäischen Union bzw. des Europäischen Wirtschaftsraums muss daher sichergestellt sein, dass auch bei einer Verarbeitung in diesen sog. Drittstaaten ein angemessenes Datenschutzniveau herrscht. Die Regelungen dazu finden sich in Kapitel 5 der DS-GVO in den Art. 44 – 50. Dabei müssen aber weiterhin die rechtlichen Voraussetzungen für die Einbeziehung eines Dienstleisters aus Art. 28 beachtet werden, das Kapitel 5 der DS-GVO regelt allein die Anforderungen an den Transfer in ein Drittland.

Die EU-Kommission kann in Angemessenheitsbeschlüssen (Art. 45) für einen Drittstaat ein angemessenes Datenschutzniveau feststellen, so hat sie dies beispielsweise für die Schweiz oder Israel getan.

Aber auch durch die Verwendung von durch die EU-Kommission festgelegten Standardvertragsklauseln (Art. 46 Abs. 2 lit. c) kann beim datenempfangenden Unternehmen ein angemessenes Datenschutzniveau hergestellt werden. Die Verpflichtung zu unternehmensweiten verbindlichen Verhaltensregeln (Art. 47), die durch eine europäische Datenschutzaufsichtsbehörde freigegeben wurden (BCR – Binding Corporate Rules) sind eine weitere Möglichkeit, einen Drittstaatentransfer rechtlich abzusichern. Durch die DS-GVO gibt es künftig auch die Variante, dies über das Vorhandensein entsprechender genehmigter Verhaltensregeln oder Zertifikate darzulegen (Art. 46 Abs. 2 lit. e und f).

Ein Sonderfall ist der Datentransfer in die USA. Ein Angemessenheitsbeschluss für die USA liegt nicht vor, aber die EU-Kommission hat sich mit der US-Regierung auf ein Abkommen über ein Zertifizierungsverfahren verständig, das den Namen EU-US Privacy Shield trägt und bei dem sich US-Unternehmen gegenüber dem US-Handelsministerium zur Einhaltung festgelegter Vorgaben verpflichten. Dieses Verfahren ist umstritten und Rechtssicherheit wird es erst nach einer Befassung des EuGH mit diesem Abkommen geben. Bis dahin ist das EU-US Privacy Shield eine zulässige Grundlage für den Datentransfer in die USA.

Durch die DS-GVO wird nun auch klargestellt, dass auch der Auftragsverarbeiter Daten in Drittländer transferieren darf (Art. 44). Meist wird dies der Fall sein, wenn bei Wartungs-/Supportsituationen ein Spezialist in Sonderfällen bei den im Rahmen der Leistung eingesetzten IT-Komponenten nur durch Fernwartung eine Fehleranalyse- oder Störungsbeseitigung durchführen kann. Durch geeignete Schutzmaßnahmen und Vereinbarungen hat der Auftragsverarbeiter dann die Zulässigkeit sicherzustellen.

5.2 Erwägungsgründe

In den Erwägungsgründen 101 - 115 finden sich Ausführungen, die zur Auslegung herangezogen werden können.

5.4 Handlungsfelder zur Drittstaatenthematik

- Beachten Sie, dass jede Verlagerung der Dienstleistung oder von vereinbarten Teilarbeiten in ein Drittland der vorherigen Zustimmung des Auftraggebers bedarf und dass dies mit Ihren Dienstleistern / Auftraggebern auch vereinbart ist.
- Erfassen Sie durch Ihren Einkauf bzw. Produktverantwortlichen die Dienstleister, die die vereinbarte Tätigkeit in einem Drittstaat erbringen und dokumentieren Sie die Rechtsgrundlage für den Datentransfer.
- Regeln Sie in Ihren Verträgen mit dem Dienstleister, ob dieser Daten in Drittstaaten transferieren darf.
- Liegen geeignete Garantien vor, z. B. Standardvertragsklauseln? Hierzu ist es empfehlenswert, den Datenschutzbeauftragten einzubeziehen, sobald eine Drittlandsverarbeitung stattfindet.

5.5. Kontrolle

- Findet die Datenverarbeitung im Auftrag in sog. Drittländern statt, sollten die aktuellen Vertragsbedingungen regelmäßig mit dem geltenden Recht der Europäischen Union abgeglichen werden, falls beispielsweise der EuGH hierzu Aussagen trifft, die Vertragsverhältnisse von Ihnen betreffen.

6. Haftung

6. 1 Einführung

Entsteht einer Person, deren personenbezogenen Daten im Rahmen einer Auftragsverarbeitung verarbeitet werden, wegen Verstoßes gegen diese Verordnung ein *materieller* oder *immaterieller* Schaden, so hat sie nach Art. 82 Abs. 1 Anspruch auf Schadenersatz. Neu ist, dass sich der Schadenersatzanspruch auch gegen den Auftragsverarbeiter als direkter Anspruch richtet. In der Diskussion ist auch, dass nach den Formulierungen des Art. 82 Abs. 4 Verantwortlicher und Auftragsverarbeiter als Gesamtschuldner haften.

Im Folgenden sollen die Erwägungsgründe, referenzierenden Artikel, Handlungsfelder und Sanktionen erläutert werden.

6.2 Erwägungsgründe zur Haftung

In den Erwägungsgründen 74, 146 und 147 finden sich Ausführungen, die zur Auslegung herangezogen werden können.

6.3 Referenzierende Artikel zur Haftung

Ausführungen zur Haftung finden sich in Artikel 82 und im Erwägungsgrund 146.

6.4 Handlungsfelder zur Haftung

1. Implementierung eines unternehmensinternen Prozesses, damit der Datenschutzbeauftragte bei externer Auftragsvergabe, bei der personenbezogene Daten verarbeitet werden, eingebunden wird, um sicherstellen zu können, dass Vereinbarungen zur Auftragsverarbeitung mit entsprechenden Haftungsregelungen geschlossen werden.

2. Es ist durch den Verantwortlichen sicherzustellen, dass die Vereinbarungen zur Auftragsverarbeitung bzw. Hauptverträge zur Leistung (Verträge) mit Auftragsverarbeitern auch bzgl. der Haftungsregelungen Art. 82 EU-DS-GVO entsprechen, d.h., Verantwortlichkeiten und Haftungsregelungen sind aufzunehmen.

3. Es empfiehlt sich, Bestandsverträge mit Laufzeit nach dem 25.05.2018 per Nachtrag anzupassen. Dazu ist zu erheben, ob mit allen Auftragsverarbeitern bereits Vereinbarungen zu Auftragsverarbeitung geschlossen sind. Entsprechende zeitliche Vorläufe sind hierbei zu beachten. Den Abteilungen sind entsprechende Nachträge zu Bestandverträgen als Muster zur Verhandlung mit den Auftragsverarbeitern vorzugeben.

4. Um möglichst im Vorfeld auszuschließen, dass es zum Schadenersatzanspruch kommt, sind die Dienstleister auswählenden Abteilungen anzuweisen, Auftragsverarbeiter je nach zu verarbeitenden Datenkategorien und Datenverarbeitung sorgfältig auszuwählen, insbesondere sich auch aktuelle Zertifikate etc. vorlegen zu lassen und dies zu dokumentieren.

5. Die denkbaren Risiken für den Verantwortlichen, aber auch für den Auftragsverarbeiter können durch die Vereinbarung zum Abschluss einer Haftpflichtversicherung abgesichert werden. Hierbei ist zu beachten, dass die Aufrechterhaltung

   - für die gesamte Vertragslaufzeit zu gewährleisten ist, und
   - die Deckungssummen im Verhältnis zu den bestehenden Risiken ausreichend sind.

   Man kann zusätzlich noch in Erwägung ziehen, sich eine Versicherungsbestätigung und den Versicherungsschein vorlegen zu lassen.

6. Bei Subunternehmereinsatz (weitere Auftragsverarbeiter) gelten vorgenannte Ausführungen zur Haftung entsprechend.

6.5 Sanktionen

Es sind in der DS-GVO keine Sanktionen vorgesehenen, wenn die Vertragsparteien keine Regelungen zur Haftung getroffen haben. Dann gelten die gesetzlichen Regelungen aus Art. 82 DS-GVO.

6.6 Kontrolle

- Gibt es ausreichende Haftungsregelungen und Regelungen zur gegenseitigen Unterstützung durch den Vertragspartner zur Abwehr von Ansprüchen Dritter?
- Sind die Haftungsrisiken durch ein Verschulden der anderen Partei durch eine adäquate Haftpflichtversicherung abgedeckt?

7. Datenpannen

7.1 Einführung

Die Meldepflicht bei Datenpannen, wie in § 42a BDSG beschrieben, findet in den Art. 33 und 34 DS-GVO ihre Nachfolger. Die beiden Artikel teilen sich die Regelungen der Voraussetzung und Umsetzung einer Meldepflicht gegenüber der Aufsichtsbehörde und der betroffenen Person auf. Im Vergleich zu § 42a BDSG wird eine Meldepflicht nun nicht mehr auf bestimmte Datenkategorien begrenzt. Voraussetzung ist eine Verletzung des Schutzes personenbezogener Daten. Was darunter zu verstehen ist wird in Art. 4 Nr. 12 DS-GVO definiert:

12. „Verletzung des Schutzes personenbezogener Daten" eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden;

Das heißt, eine Schutzverletzung ohne Folgen, wird von einer Meldepflicht nicht umfasst. Für eine Meldepflicht an die Aufsichtsbehörde ist erforderlich, dass diese Schutzverletzung zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Dann ist die Aufsichtsbehörde innerhalb von 72 Stunden zu informieren. Eine Meldung nach dieser Frist ist zu begründen. Art. 33 Abs. 3 DS-GVO gibt die dabei erforderlichen Informationen vor. Auf der Homepage des BayLDA gibt es hier bereits die Möglichkeit, eine Datenpanne online zu melden. (Link zur Seite: (https://www.lda.bayern.de/de/datenpanne.html)

Bei der Benachrichtigungspflicht einer natürlichen Person variieren die Voraussetzungen:

Hier muss die Schutzverletzung voraussichtlich zu einem hohen Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen führen. Die Benachrichtigung selbst hat unverzüglich und in einer klaren und einfachen Sprache zu erfolgen und orientiert sich an den Inhalten, die auch der Aufsichtsbehörde zu melden sind.

7.2 Erwägungsgründe zu Datenpannen

In den Erwägungsgründen 85 - 88 finden sich Ausführungen, die zur Auslegung herangezogen werden können.

7.3 Handlungsfelder zu Datenpannen

Handlungsfelder

- Informieren Sie intern über die neuen Anforderungen und definieren Sie mit den betroffenen Bereichen oder unternehmensübergreifend Prozesse zum Umgang zur Dokumentation und Bearbeitung (einschließlich ggf. zu treffender Maßnahmen) von Vorfällen.
- Entwerfen Sie gemeinsam mit den betroffenen Bereichen Beispielsfälle und schulen Sie die zuständigen Mitarbeiter.
- Informieren Sie sich über die Meldewege bei Ihrer zuständigen Aufsichtsbehörde.
- Definieren Sie, wer im Unternehmen die Meldung übernimmt (für ausreichende Vertretung aufgrund der 72-Stunden-Frist Sorge tragen).
- Binden Sie den Einkauf bzw. Produktverantwortliche ein, damit Auftragsverarbeiter auf die geänderten Anforderungen und Prozesse zu Subunternehmern hingewiesen werden.

- Prüfen Sie bestehende Vereinbarungen zur Auftragsverarbeitung, ob bereits Regelungen getroffen sind, die eine zeitnahe Information des Auftragsgebers bei meldepflichtigen Schutzverletzungen sicherstellen.

7.4 Sanktionen

In Art. 83 Abs. 4 lit. a) DS-GVO werden Verstöße gegen die Vorgaben zur Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde bzw. von Verstößen gegen die Benachrichtigungspflicht der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person gegenüber dem Verantwortlichen mit Geldbuße bis 10 Mio. Euro oder 2 % des weltweiten Jahresumsatzes sanktioniert, je nachdem welcher der Beträge höher ist.

7.5 Kontrolle

- Installieren Sie interne Prozesse zur Meldung von Schutzverletzung, die auch Meldungen durch den Auftragsverarbeiter beinhalten.
- Verpflichten Sie den Auftragsverarbeiter zur Meldung bei Schutzverletzung, die zu den Rechtsfolgen des Art. 33 oder 34 führen können.

8. Anhang

8.1 Relevante Artikel aus der DS-GVO (ohne Kapitel V)

Artikel 5 Abs. 1 lit. f:

Personenbezogene Daten müssen (...) in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit");

Artikel 5 Abs. 2

(2) Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können („Rechenschaftspflicht").

Artikel 28 Auftragsverarbeiter

(1) Erfolgt eine Verarbeitung im Auftrag eines Verantwortlichen, so arbeitet dieser nur mit Auftragsverarbeitern, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.

(2) Der Auftragsverarbeiter nimmt keinen weiteren Auftragsverarbeiter ohne vorherige gesonderte oder allgemeine schriftliche Genehmigung des Verantwortlichen in Anspruch. Im Fall einer allgemeinen schriftlichen Genehmigung informiert der Auftragsverarbeiter den Verantwortlichen immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter, wodurch der Verantwortliche die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben.

(3) Die Verarbeitung durch einen Auftragsverarbeiter erfolgt auf der Grundlage eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, der bzw. das den Auftragsverarbeiter in Bezug auf den Verantwortlichen bindet und in dem Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Pflichten und Rechte des Verantwortlichen festgelegt sind. Dieser Vertrag bzw. dieses andere Rechtsinstrument sieht insbesondere vor, dass der Auftragsverarbeiter

a) die personenbezogenen Daten nur auf dokumentierte Weisung des Verantwortlichen – auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation – verarbeitet, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist; in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet;
b) gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen[12];
c) alle gemäß Artikel 32 erforderlichen Maßnahmen ergreift;
d) die in den Absätzen 2 und 4 genannten Bedingungen für die Inanspruchnahme der Dienste eines weiteren Auftragsverarbeiters einhält;

[12] Zu beachten ist, dass die Datenverarbeitung im Auftrag auch künftig keine Erlaubnis darstellt, Daten dem Auftragsverarbeiter zu offenbaren, die aufgrund gesetzlicher Geheimhaltungspflichten oder von Berufs- oder besonderen Amtsgeheimnissen, die nicht auf gesetzlichen Vorschriften beruhen, vertraulich zu behandeln sind (vgl. § 1 Abs. 2 S. 3 BDSG-neu).

e) angesichts der Art der Verarbeitung den Verantwortlichen nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützt, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III genannten Rechte der betroffenen Person nachzukommen;
f) unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen bei der Einhaltung der in den Artikeln 32 bis 36 genannten Pflichten unterstützt;
g) nach Abschluss der Erbringung der Verarbeitungsleistungen alle personenbezogenen Daten nach Wahl des Verantwortlichen entweder löscht oder zurückgibt, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht;
h) dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in diesem Artikel niedergelegten Pflichten zur Verfügung stellt und Überprüfungen — einschließlich Inspektionen –, die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, ermöglicht und dazu beiträgt.

Mit Blick auf Unterabsatz 1 Buchstabe h informiert der Auftragsverarbeiter den Verantwortlichen unverzüglich, falls er der Auffassung ist, dass eine Weisung gegen diese Verordnung oder gegen andere Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstößt.

(4) Nimmt der Auftragsverarbeiter die Dienste eines weiteren Auftragsverarbeiters in Anspruch, um bestimmte Verarbeitungstätigkeiten im Namen des Verantwortlichen auszuführen, so werden diesem weiteren Auftragsverarbeiter im Wege eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht des betreffenden Mitgliedstaats dieselben Datenschutzpflichten auferlegt, die in dem Vertrag oder anderen Rechtsinstrument zwischen dem Verantwortlichen und dem Auftragsverarbeiter gemäß Absatz 3 festgelegt sind, wobei insbesondere hinreichende Garantien dafür geboten werden muss, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen dieser Verordnung erfolgt. Kommt der weitere Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der erste Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten jenes anderen Auftragsverarbeiters.

(5) Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 durch einen Auftragsverarbeiter kann als Faktor herangezogen werden, um hinreichende Garantien im Sinne der Absätze 1 und 4 des vorliegenden Artikels nachzuweisen.

(6) Unbeschadet eines individuellen Vertrags zwischen dem Verantwortlichen und dem Auftragsverarbeiter kann der Vertrag oder das andere Rechtsinstrument im Sinne der Absätze 3 und 4 des vorliegenden Artikels ganz oder teilweise auf den in den Absätzen 7 und 8 des vorliegenden Artikels genannten Standardvertragsklauseln beruhen, auch wenn diese Bestandteil einer dem Verantwortlichen oder dem Auftragsverarbeiter gemäß den Artikeln 42 und 43 erteilten Zertifizierung sind.

(7) Die Kommission kann im Einklang mit dem Prüfverfahren gemäß Artikel 87 Absatz 2 Standardvertragsklauseln zur Regelung der in den Absätzen 3 und 4 des vorliegenden Artikels genannten Fragen festlegen.

(8) Eine Aufsichtsbehörde kann im Einklang mit dem Kohärenzverfahren gemäß Artikel 63 Standardvertragsklauseln zur Regelung der in den Absätzen 3 und 4 des vorliegenden Artikels genannten Fragen festlegen.

(9) Der Vertrag oder das andere Rechtsinstrument im Sinne der Absätze 3 und 4 ist schriftlich abzufassen, was auch in einem elektronischen Format erfolgen kann.

(10) Unbeschadet der Artikel 82, 83 und 84 gilt ein Auftragsverarbeiter, der unter Verstoß gegen diese Verordnung die Zwecke und Mittel der Verarbeitung bestimmt, in Bezug auf diese Verarbeitung als Verantwortlicher.

Artikel 29 Verarbeitung unter der Aufsicht des Verantwortlichen oder des Auftragsverarbeiters

Der Auftragsverarbeiter und jede dem Verantwortlichen oder dem Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich auf Weisung des Verantwortlichen verarbeiten, es sei denn, dass sie nach dem Unionsrecht oder dem Recht der Mitgliedstaaten zur Verarbeitung verpflichtet sind.

Artikel 32 Sicherheit der Verarbeitung

(1) Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein:

a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten;
b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Artikel 82 Haftung und Recht auf Schadenersatz

(1) Jede Person, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist, hat Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter.

(2) Jeder an einer Verarbeitung beteiligte Verantwortliche haftet für den Schaden, der durch eine nicht dieser Verordnung entsprechende Verarbeitung verursacht wurde. Ein Auftragsverarbeiter haftet für den durch eine Verarbeitung verursachten Schaden nur dann, 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.

(3) Der Verantwortliche oder der Auftragsverarbeiter wird von der Haftung gemäß Absatz 2 befreit, wenn er nachweist, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist.

(4) Ist mehr als ein Verantwortlicher oder mehr als ein Auftragsverarbeiter bzw. sowohl ein Verantwortlicher als auch ein Auftragsverarbeiter an derselben Verarbeitung beteiligt und sind sie gemäß den Absätzen 2 und 3 für einen durch die Verarbeitung verursachten Schaden verantwortlich, so haftet jeder Verantwortliche oder jeder Auftragsverarbeiter für den gesamten Schaden, damit ein wirksamer Schadensersatz für die betroffene Person sichergestellt ist.

(5) Hat ein Verantwortlicher oder Auftragsverarbeiter gemäß Absatz 4 vollständigen Schadenersatz für den erlittenen Schaden gezahlt, so ist dieser Verantwortliche oder Auftragsverarbeiter berechtigt, von den übrigen an derselben Verarbeitung beteiligten für die Datenverarbeitung Verantwortlichen oder Auftragsverarbeitern den Teil des Schadenersatzes zurückzufordern, der unter den in Absatz 2 festgelegten Bedingungen ihrem Anteil an der Verantwortung für den Schaden entspricht.

(6) Mit Gerichtsverfahren zur Inanspruchnahme des Rechts auf Schadenersatz sind die Gerichte zu befassen, die nach den in Artikel 79 Absatz 2 genannten Rechtsvorschriften des Mitgliedstaats zuständig sind.

Artikel 83 Allgemeine Bedingungen für die Verhängung von Geldbußen

(1) Jede Aufsichtsbehörde stellt sicher, dass die Verhängung von Geldbußen gemäß diesem Artikel für Verstöße gegen diese Verordnung gemäß den Absätzen 5 und 6 in jedem Einzelfall wirksam, verhältnismäßig und abschreckend ist.

(2) Geldbußen werden je nach den Umständen des Einzelfalls zusätzlich zu oder anstelle von Maßnahmen nach Artikel 58 Absatz 2 Buchstaben a bis h und i verhängt. Bei der Entscheidung über die Verhängung einer Geldbuße und über deren Betrag wird in jedem Einzelfall Folgendes gebührend berücksichtigt:

a) Art, Schwere und Dauer des Verstoßes unter Berücksichtigung der Art, des Umfangs oder des Zwecks der betreffenden Verarbeitung sowie der Zahl der von der Verarbeitung betroffenen Personen und des Ausmaßes des von ihnen erlittenen Schadens;
b) Vorsätzlichkeit oder Fahrlässigkeit des Verstoßes;
c) jegliche von dem Verantwortlichen oder dem Auftragsverarbeiter getroffenen Maßnahmen zur Minderung des den betroffenen Personen entstandenen Schadens;'
d) Grad der Verantwortung des Verantwortlichen oder des Auftragsverarbeiters unter Berücksichtigung der von ihnen gemäß den Artikeln 25 und 32 getroffenen technischen und organisatorischen Maßnahmen;
e) etwaige einschlägige frühere Verstöße des Verantwortlichen oder des Auftragsverarbeiters;
f) Umfang der Zusammenarbeit mit der Aufsichtsbehörde, um dem Verstoß abzuhelfen und seine möglichen nachteiligen Auswirkungen zu mindern;
g) Kategorien personenbezogener Daten, die von dem Verstoß betroffen sind;
h) Art und Weise, wie der Verstoß der Aufsichtsbehörde bekannt wurde, insbesondere ob und gegebenenfalls in welchem Umfang der Verantwortliche oder der Auftragsverarbeiter den Verstoß mitgeteilt hat;
i) Einhaltung der nach Artikel 58 Absatz 2 früher gegen den für den betreffenden Verantwortlichen oder Auftragsverarbeiter in Bezug auf denselben Gegenstand angeordneten Maßnahmen, wenn solche Maßnahmen angeordnet wurden;
j) Einhaltung von genehmigten Verhaltensregeln nach Artikel 40 oder genehmigten Zertifizierungsverfahren nach Artikel 42 und
k) jegliche anderen erschwerenden oder mildernden Umstände im jeweiligen Fall, wie unmittelbar oder mittelbar durch den Verstoß erlangte finanzielle Vorteile oder vermiedene Verluste.

(3) Verstößt ein Verantwortlicher oder ein Auftragsverarbeiter bei gleichen oder miteinander verbundenen Verarbeitungsvorgängen vorsätzlich oder fahrlässig gegen mehrere Bestimmungen dieser Verordnung, so übersteigt der Gesamtbetrag der Geldbuße nicht den Betrag für den schwerwiegendsten Verstoß.

(4) Bei Verstößen gegen die folgenden Bestimmungen werden im Einklang mit Absatz 2 Geldbußen von bis zu 10 000 000 EUR oder im Fall eines Unternehmens von bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist:

a) die Pflichten der Verantwortlichen und der Auftragsverarbeiter gemäß den Artikeln 8, 11, 25 bis 39, 42 und 43;
b) die Pflichten der Zertifizierungsstelle gemäß den Artikeln 42 und 43;
c) die Pflichten der Überwachungsstelle gemäß Artikel 41 Absatz 4.

(5) Bei Verstößen gegen die folgenden Bestimmungen werden im Einklang mit Absatz 2 Geldbußen von bis zu 20 000 000 EUR oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist:

a) die Grundsätze für die Verarbeitung, einschließlich der Bedingungen für die Einwilligung, gemäß den Artikeln 5, 6, 7 und 9;
b) die Rechte der betroffenen Person gemäß den Artikeln 12 bis 22;
c) die Übermittlung personenbezogener Daten an einen Empfänger in einem Drittland oder an eine internationale Organisation gemäß den Artikeln 44 bis 49;
d) alle Pflichten gemäß den Rechtsvorschriften der Mitgliedstaaten, die im Rahmen des Kapitels IX erlassen wurden;

e) Nichtbefolgung einer Anweisung oder einer vorübergehenden oder endgültigen Beschränkung oder Aussetzung der Datenübermittlung durch die Aufsichtsbehörde gemäß Artikel 58 Absatz 2 oder Nichtgewährung des Zugangs unter Verstoß gegen Artikel 58 Absatz 1.

(6) Bei Nichtbefolgung einer Anweisung der Aufsichtsbehörde gemäß Artikel 58 Absatz 2 werden im Einklang mit Absatz 2 des vorliegenden Artikels Geldbußen von bis zu 20 000 000 EUR oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist.

(7) Unbeschadet der Abhilfebefugnisse der Aufsichtsbehörden gemäß Artikel 58 Absatz 2 kann jeder Mitgliedstaat Vorschriften dafür festlegen, ob und in welchem Umfang gegen Behörden und öffentliche Stellen, die in dem betreffenden Mitgliedstaat niedergelassen sind, Geldbußen verhängt werden können.

(8) Die Ausübung der eigenen Befugnisse durch eine Aufsichtsbehörde gemäß diesem Artikel muss angemessenen Verfahrensgarantien gemäß dem Unionsrecht und dem Recht der Mitgliedstaaten, einschließlich wirksamer gerichtlicher Rechtsbehelfe und ordnungsgemäßer Verfahren, unterliegen.

(9) Sieht die Rechtsordnung eines Mitgliedstaats keine Geldbußen vor, kann dieser Artikel so angewandt werden, dass die Geldbuße von der zuständigen Aufsichtsbehörde in die Wege geleitet und von den zuständigen nationalen Gerichten verhängt wird, wobei sicherzustellen ist, dass diese Rechtsbehelfe wirksam sind und die gleiche Wirkung wie die von Aufsichtsbehörden verhängten Geldbußen haben. In jeden Fall müssen die verhängten Geldbußen wirksam, verhältnismäßig und abschreckend sein. Die betreffenden Mitgliedstaaten teilen der Kommission bis zum 25. Mai 2018 die Rechtsvorschriften mit, die sie aufgrund dieses Absatzes erlassen, sowie unverzüglich alle späteren Änderungsgesetze oder Änderungen dieser Vorschriften.

Artikel 84 Sanktionen

(1) Die Mitgliedstaaten legen die Vorschriften über andere Sanktionen für Verstöße gegen diese Verordnung – insbesondere für Verstöße, die keiner Geldbuße gemäß Artikel 83 unterliegen – fest und treffen alle zu deren Anwendung erforderlichen Maßnahmen. Diese Sanktionen müssen wirksam, verhältnismäßig und abschreckend sein.

(2) Jeder Mitgliedstaat teilt der Kommission bis zum 25. Mai 2018 die Rechtsvorschriften, die er aufgrund von Absatz 1 erlässt, sowie unverzüglich alle späteren Änderungen dieser Vorschriften mit.

8.2 Relevante Erwägungsgründe aus der DS-GVO

Erwägungsgrund 74 (Art. 82 Abs. 1)

Die Verantwortung und Haftung des Verantwortlichen für jedwede Verarbeitung personenbezogener Daten, die durch ihn oder in seinem Namen erfolgt, sollte geregelt werden. Insbesondere sollte der der Verantwortliche geeignete und wirksame Maßnahmen treffen müssen und nachweisen können, dass die Verarbeitungstätigkeiten im Einklang mit dieser Verordnung stehen und die Maßnahmen auch wirksam sind. Dabei sind Art, Umfang, Umstände und Verarbeitungszwecke und das Risiko für die Rechte und Freiheiten natürlicher Personen berücksichtigen.

Erwägungsgrund 81

Damit die Anforderungen dieser Verordnung in Bezug auf die vom Auftragsverarbeiter im Namen des Verantwortlichen vorzunehmende Verarbeitung eingehalten werden, sollte ein Verantwortlicher, der einen Auftragsverarbeiter mit Verarbeitungstätigkeiten betrauen will, nur Auftragsverarbeiter heranziehen, die – insbesondere im Hinblick auf Fachwissen, Zuverlässigkeit und Ressourcen – hinreichende Garantien dafür bieten, dass technische und organisatorische Maßnahmen – auch für die Sicherheit der Verarbeitung – getroffen werden, die den Anforderungen dieser Verordnung genügen. Die Einhaltung genehmigter Verhaltensregeln oder eines genehmigten Zertifizierungsverfahrens durch einen Auftragsverarbeiter kann als Faktor

herangezogen werden, um die Erfüllung der Pflichten des Verantwortlichen nachzuweisen. Die Durchführung einer Verarbeitung durch einen Auftragsverarbeiter sollte auf Grundlage eines Vertrags oder eines anderen Rechtsinstruments nach dem Recht der Union oder der Mitgliedstaaten erfolgen, der bzw. das den Auftragsverarbeiter an den Verantwortlichen bindet und in dem Gegenstand und Dauer der Verarbeitung, Art und Zwecke der Verarbeitung, die Art der personenbezogenen Daten und die Kategorien von betroffenen Personen festgelegt sind, wobei die besonderen Aufgaben und Pflichten des Auftragsverarbeiters bei der geplanten Verarbeitung und das Risiko für die Rechte und Freiheiten der betroffenen Person zu berücksichtigen sind. Der Verantwortliche und der Auftragsverarbeiter können entscheiden, ob sie einen individuellen Vertrag oder Standardvertragsklauseln verwenden, die entweder unmittelbar von der Kommission erlassen oder aber nach dem Kohärenzverfahren von einer Aufsichtsbehörde angenommen und dann von der Kommission erlassen wurden. Nach Beendigung der Verarbeitung im Namen des Verantwortlichen sollte der Auftragsverarbeiter die personenbezogenen Daten nach Wahl des Verantwortlichen entweder zurückgeben oder löschen, sofern nicht nach dem Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht.

Erwägungsgrund 85

Eine Verletzung des Schutzes personenbezogener Daten kann – wenn nicht rechtzeitig und angemessen reagiert wird – einen physischen, materiellen oder immateriellen Schaden für natürliche Personen nach sich ziehen, wie etwa Verlust der Kontrolle über ihre personenbezogenen Daten oder Einschränkung ihrer Rechte, Diskriminierung, Identitätsdiebstahl oder -betrug, finanzielle Verluste, unbefugte Aufhebung der Pseudonymisierung, Rufschädigung, Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Daten oder andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile für die betroffene natürliche Person. Deshalb sollte der Verantwortliche, sobald ihm eine Verletzung des Schutzes personenbezogener Daten bekannt wird, die Aufsichtsbehörde von der Verletzung des Schutzes personenbezogener Daten unverzüglich und, falls möglich, binnen höchstens 72 Stunden, nachdem ihm die Verletzung bekannt wurde, unterrichten, es sei denn, der Verantwortliche kann im Einklang mit dem Grundsatz der Rechenschaftspflicht nachweisen, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen führt. Falls diese Benachrichtigung nicht binnen 72 Stunden erfolgen kann, sollten in ihr die Gründe für die Verzögerung angegeben werden müssen, und die Informationen können schrittweise ohne unangemessene weitere Verzögerung bereitgestellt werden.

Erwägungsgrund 86

Der für die Verarbeitung Verantwortliche sollte die betroffene Person unverzüglich von der Verletzung des Schutzes personenbezogener Daten benachrichtigen, wenn diese Verletzung des Schutzes personenbezogener Daten voraussichtlich zu einem hohen Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen führt, damit diese die erforderlichen Vorkehrungen treffen können. Die Benachrichtigung sollte eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten sowie an die betroffene natürliche Person gerichtete Empfehlungen zur Minderung etwaiger nachteiliger Auswirkungen dieser Verletzung enthalten. Solche Benachrichtigungen der betroffenen Person sollten stets so rasch wie nach allgemeinem Ermessen möglich, in enger Absprache mit der Aufsichtsbehörde und nach Maßgabe der von dieser oder von anderen zuständigen Behörden wie beispielsweise Strafverfolgungsbehörden erteilten Weisungen erfolgen. Um beispielsweise das Risiko eines unmittelbaren Schadens mindern zu können, müssten betroffene Personen sofort benachrichtigt werden, wohingegen eine längere Benachrichtigungsfrist gerechtfertigt sein kann, wenn es darum geht, geeignete Maßnahmen gegen fortlaufende oder vergleichbare Verletzungen des Schutzes personenbezogener Daten zu treffen.

Erwägungsgrund 87

Es sollte festgestellt werden, ob alle geeigneten technischen Schutz- sowie organisatorischen Maßnahmen getroffen wurden, um sofort feststellen zu können, ob eine Verletzung des Schutzes personenbezogener Daten aufgetreten ist, und um die Aufsichtsbehörde und die betroffene Person umgehend unterrichten zu können. Bei der Feststellung, ob die Meldung unverzüglich erfolgt ist, sollten die Art und Schwere der Ver-

letzung des Schutzes personenbezogener Daten sowie deren Folgen und nachteilige Auswirkungen für die betroffene Person berücksichtigt werden. Die entsprechende Meldung kann zu einem Tätigwerden der Aufsichtsbehörde im Einklang mit ihren in dieser Verordnung festgelegten Aufgaben und Befugnissen führen.

Erwägungsgrund 88

Bei der detaillierten Regelung des Formats und der Verfahren für die Meldung von Verletzungen des Schutzes personenbezogener Daten sollten die Umstände der Verletzung hinreichend berücksichtigt werden, beispielsweise ob personenbezogene Daten durch geeignete technische Sicherheitsvorkehrungen geschützt waren, die die Wahrscheinlichkeit eines Identitätsbetrugs oder anderer Formen des Datenmissbrauchs wirksam verringern. Überdies sollten solche Regeln und Verfahren den berechtigten Interessen der Strafverfolgungsbehörden in Fällen Rechnung tragen, in denen die Untersuchung der Umstände einer Verletzung des Schutzes personenbezogener Daten durch eine frühzeitige Offenlegung in unnötiger Weise behindert würde.

Erwägungsgrund 95 (für Art. 28 (3) f)

Der Auftragsverarbeiter sollte erforderlichenfalls den Verantwortlichen auf Anfrage bei der Gewährleistung der Einhaltung der sich aus der Durchführung der Datenschutz-Folgenabschätzung und der vorherigen Konsultation der Aufsichtsbehörde ergebenden Auflagen unterstützen.

Erwägungsgrund 98

Verbände oder andere Vereinigungen, die bestimmte Kategorien von Verantwortlichen oder Auftragsverarbeitern vertreten, sollten ermutigt werden, in den Grenzen dieser Verordnung Verhaltensregeln auszuarbeiten, um eine wirksame Anwendung dieser Verordnung zu erleichtern, wobei den Besonderheiten der in bestimmten Sektoren erfolgenden Verarbeitungen und den besonderen Bedürfnissen der Kleinunternehmen sowie der kleinen und mittleren Unternehmen Rechnung zu tragen ist. Insbesondere könnten in diesen Verhaltensregeln - unter Berücksichtigung des mit der Verarbeitung wahrscheinlich einhergehenden Risikos für die Rechte und Freiheiten natürlicher Personen - die Pflichten der Verantwortlichen und der Auftragsverarbeiter bestimmt werden.

Erwägungsgrund 101

Der Fluss personenbezogener Daten aus Drittländern und internationalen Organisationen und in Drittländer und internationale Organisationen ist für die Ausweitung des internationalen Handels und der internationalen Zusammenarbeit notwendig. Durch die Zunahme dieser Datenströme sind neue Herausforderungen und Anforderungen in Bezug auf den Schutz personenbezogener Daten entstanden. Das durch diese Verordnung unionsweit gewährleistete Schutzniveau für natürliche Personen sollte jedoch bei der Übermittlung personenbezogener Daten aus der Union an Verantwortliche, Auftragsverarbeiter oder andere Empfänger in Drittländern oder an internationale Organisationen nicht untergraben werden, und zwar auch dann nicht, wenn aus einem Drittland oder von einer internationalen Organisation personenbezogene Daten an Verantwortliche oder Auftragsverarbeiter in demselben oder einem anderen Drittland oder an dieselbe oder eine andere internationale Organisation weiterübermittelt werden. In jedem Fall sind derartige Datenübermittlungen an Drittländer und internationale Organisationen nur unter strikter Einhaltung dieser Verordnung zulässig. Eine Datenübermittlung könnte nur stattfinden, wenn die in dieser Verordnung festgelegten Bedingungen zur Übermittlung personenbezogener Daten an Drittländer oder internationale Organisationen vorbehaltlich der übrigen Bestimmungen dieser Verordnung von dem Verantwortlichen oder dem Auftragsverarbeiter erfüllt werden.

Erwägungsgrund 146

Der Verantwortliche oder der Auftragsverarbeiter sollte Schäden, die einer Person aufgrund einer Verarbeitung entstehen, die mit dieser Verordnung nicht im Einklang steht, ersetzen. Der Verantwortliche oder der Auftragsverarbeiter sollte von seiner Haftung befreit werden, wenn er nachweist, dass er in keiner Weise für den Schaden verantwortlich ist. Der Begriff des Schadens sollte im Lichte der Rechtsprechung des Gerichts-

hofs weit auf eine Art und Weise ausgelegt werden, die den Zielen dieser Verordnung in vollem Umfang entspricht. Dies gilt unbeschadet von Schadenersatzforderungen aufgrund von Verstößen gegen andere Vorschriften des Unionsrechts oder des Rechts der Mitgliedstaaten. Zu einer Verarbeitung, die mit der vorliegenden Verordnung nicht im Einklang steht, zählt auch eine Verarbeitung, die nicht mit den nach Maßgabe der vorliegenden Verordnung erlassenen delegierten Rechtsakten und Durchführungsrechtsakten und Rechtsvorschriften der Mitgliedstaaten zur Präzisierung von Bestimmungen der vorliegenden Verordnung im Einklang steht. Die betroffenen Personen sollten einen vollständigen und wirksamen Schadenersatz für den erlittenen Schaden erhalten. Sind Verantwortliche oder Auftragsverarbeiter an derselben Verarbeitung beteiligt, so sollte jeder Verantwortliche oder Auftragsverarbeiter für den gesamten Schaden haftbar gemacht werden. Werden sie jedoch nach Maßgabe des Rechts der Mitgliedstaaten zu demselben Verfahren hinzugezogen, so können sie im Verhältnis zu der Verantwortung anteilmäßig haftbar gemacht werden, die jeder Verantwortliche oder Auftragsverarbeiter für den durch die Verarbeitung entstandenen Schaden zu tragen hat, sofern sichergestellt ist, dass die betroffene Person einen vollständigen und wirksamen Schadenersatz für den erlittenen Schaden erhält. Jeder Verantwortliche oder Auftragsverarbeiter, der den vollen Schadenersatz geleistet hat, kann anschließend ein Rückgriffsverfahren gegen andere an derselben Verarbeitung beteiligte Verantwortliche oder Auftragsverarbeiter anstrengen.

Erwägungsgrund 147

Soweit in dieser Verordnung spezifische Vorschriften über die auf Verfahren im Hinblick auf einen gerichtlichen Rechtsbehelf einschließlich Schadenersatz gegen einen Verantwortlichen oder Auftragsverarbeiter — enthalten sind, sollten die allgemeinen Vorschriften über die Gerichtsbarkeit, wie sie etwa in der Verordnung (EU) Nr. 1215/2012 des Europäischen Parlaments und des Rates (13) enthalten sind, der Anwendung dieser spezifischen Vorschriften nicht entgegenstehen.