Der Bayerische Landesbeauftragte
für den Datenschutz

Auftragsverarbeitung

Orientierungshilfe

Herausgeber:

Der Bayerische Landesbeauftragte für den Datenschutz
80538 München | Wagmüllerstraße 18
Telefon: +49 89 21 26 72-0
E-Mail: poststelle@datenschutz-bayern.de
https://www.datenschutz-bayern.de

Bearbeiter:

Dr. Sebastian Müller | Dr. Matthias Stief

Redaktion:

Dr. Kai Engelbrecht

Version 2.0 | Stand: 1. April 2019

Diese Orientierungshilfe wird ausschließlich in elektronischer Form bereitgestellt. Sie kann im Internet auf https://www.datenschutz-bayern.de in der Rubrik „Datenschutzreform 2018“ abgerufen werden.

Die PDF-Datei ist für den doppelseitigen Ausdruck optimiert.

Vorwort

Die Datenschutz-Grundverordnung (DSGVO) gilt seit dem 25. Mai 2018. Sie fasst unter anderem die Regeln zur Auftragsverarbeitung (bisher: Auftragsdatenverarbeitung) neu. Die Neuregelung lässt viele der schon bisher geltenden Anforderungen an den Verantwortlichen im Wesentlichen unverändert. Für den Auftragsverarbeiter ergeben sich vor allem Änderungen seiner datenschutzrechtlichen Verantwortlichkeit und Haftung.

Diese Orientierungshilfe stellt praktische und rechtliche Gesichtspunkte der Auftragsverarbeitung ohne Anspruch auf Vollständigkeit und unter dem Vorbehalt der weiteren Rechtsentwicklung auf nationaler und europäischer Ebene dar.

Auf Verarbeitungen im Anwendungsbereich der Datenschutz-Richtlinie für Polizei und Strafjustiz[1] findet die Datenschutz-Grundverordnung keine unmittelbare Anwendung (vgl. Art. 2 Abs. 2 Buchst. d DSGVO), sie wird aber in Umsetzung der Datenschutz-Richtlinie für Polizei und Strafjustiz in weiten Teilen für anwendbar erklärt (vgl. Art. 2 Satz 1, Art. 28 ff. des Bayerischen Datenschutzgesetzes – BayDSG). Besonderheiten der Regelungen im Anwendungsbereich der Datenschutz-Richtlinie für Polizei und Strafjustiz sind in diesem Papier durch ein blaues Polizeiauto gekennzeichnet. Die Regelungen im Bayerischen Datenschutzgesetz zur Anwendbarkeit der Datenschutz-Grundverordnung in diesem Bereich werden nur bei materiellen Abweichungen zitiert.

[1] Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl. L 119 vom 4. Mai 2016, S. 89).

Inhaltsverzeichnis

1. Allgemeines

a) Praktische Bedeutung und Erscheinungsformen der Auftragsverarbeitung

Auftragsverarbeitung im Sinne des Datenschutzrechts bedeutet die Verarbeitung personenbezogener Daten durch einen Auftragsverarbeiter (regelmäßig ein entsprechender Dienstleister) im Auftrag des Verantwortlichen. Die Auftragsverarbeitung erleichtert arbeitsteiliges Handeln. Dabei wird dem Auftragsverarbeiter nicht die eigentliche (Verwaltungs-) Aufgabe übertragen, sondern nur eine Hilfstätigkeit.

Auftragsverarbeitung ist nicht nur in der Privatwirtschaft, sondern auch in der öffentlichen Verwaltung verbreitet. Insbesondere kleinere Behörden oder Kommunen verfügen häufig nicht über ausreichende personelle Kapazitäten, um den zunehmenden Betreuungsaufwand von immer mehr Daten, immer komplexeren Verfahren und sich rasant weiterentwickelnden Technologien selbst zu bewältigen. Vor allem in Zeiten von Personalknappheit erleichtert das Einschalten von spezialisierten Dienstleistern die Abwicklung von Routine- und Massentätigkeiten, aber auch die Durchführung technisch anspruchsvoller Vorhaben.

Generell ist bei der Beauftragung eines externen Dienstleisters gedanklich zu prüfen, ob diesem die Möglichkeit zum Zugriff auf personenbezogene Daten eingeräumt wird. Das kann bei der Erstellung von Namensschildern oder der Verwaltung und Ausgabe von namentlich beschrifteter Bekleidung, etwa in einem Krankenhaus, der Fall sein. Je nach Ausgestaltung des Outsourcings sind die Regelungen zur Auftragsverarbeitung direkt oder entsprechend (vgl. Art. 5 Abs. 3 BayDSG) anwendbar. Dagegen liegt keine Auftragsverarbeitung vor, wenn kein Zugriff auf personenbezogene Daten des Auftraggebers möglich ist. Die einschlägigen Konstellationen lassen sich im Rahmen dieser Orientierungshilfe nicht annähernd erschöpfend darstellen.

Die Auftragsverarbeitung kann sowohl innerhalb der Räume des Verantwortlichen als auch außerhalb stattfinden. Typische Beispiele sind:

- **Erledigung von Massenarbeiten**

  Weit verbreitet ist der Versand von Mitteilungsblättern, Informationsbroschüren, Beitragsrechnungen und sonstigen Drucksachen durch einen Dienstleister auf der Basis eines vom Verantwortlichen zur Verfügung gestellten Adressenbestandes.

- **Datenerfassung, Datenumsetzung und Scannen von Dokumenten**

  Ein typisches Beispiel für eine extern vergebene Datenverarbeitungsaufgabe ist das Einscannen von Dokumenten. Auch die Verfilmung von Daten auf Papier und Mikrofiches oder eine Übertragung der Daten von magnetischen Datenträgern auf optische Speichermedien (Erstellen von CD-ROMs und DVDs) kommt als Auftragsverarbeitung in Betracht.

1. Allgemeines

▶ Outsourcing im klassischen Sinn

Im Vordringen ist das Auslagern von Versandarbeiten („ePost“). Auch das Vorhalten von Backup-Kapazitäten für den Katastrophenfall ist heute noch ein klassisches Feld der Auftragsverarbeitung. Viele Behörden und Kommunen bedienen sich für ihre Datenverarbeitungsaktivitäten eines einzigen Rechenzentrums oder Serverraums. Für den Katastrophenfall weicht man häufig auf ein (mobiles) Backup-Rechenzentrum eines Dienstleisters oder des Herstellers aus.

Häufig werden Teile der Bürokommunikation ausgelagert. So übernehmen externe Dienstleister etwa die Beschaffung, Installation und Betreuung der entsprechenden Software (z. B. Textverarbeitung, E-Mail-Kommunikation) oder von Hardware. Gründe hierfür sind neben Wirtschaftlichkeitsüberlegungen das fehlende eigene Fachpersonal und die Schaffung einheitlicher Standards für alle Arbeitsplätze. Bestandteil ist in der Regel auch die Einrichtung eines so genannten User-Help-Desks, den die Anwender bei Auftreten von Problemen zu Rate ziehen können.

▶ Cloud Computing

Cloud Computing ist eine moderne Form von Outsourcing. Dabei werden einzelne oder auch mehrere Datenverarbeitungsvorgänge in die sogenannte Cloud (engl. für Wolke) ausgelagert. Die Cloud besteht aus Rechnerlandschaften, die von externen Anbietern vor allem über das Internet bereitgestellt werden. Der Anwendungsbereich reicht von der Nutzung extern bereitgestellter (Spezial-)Software oder Speicherkapazitäten bis hin zur Auslagerung der gesamten IT-Infrastruktur.

▶ Programmerstellung

Gelegentlich werden auch Programmieraufträge an Dritte vergeben, etwa die Entwicklung sogenannter „Apps“. Das ist vor allem dann angezeigt, wenn die eigene Behörde nicht über das (vorübergehend) benötigte technische Know-How verfügt. Verbunden wird dies häufig mit Wartungsverträgen.

▶ Durchführung von Befragungen und Forschungsaufträgen

Insbesondere im Forschungsbereich werden häufig Befragungsaktionen und deren Auswertungen an dafür spezialisierte Institute vergeben.

▶ Archivierung von Daten

Bei der Archivierung von maschinenlesbaren Datenträgern sowie von Altakten, auf die nicht mehr ständig zugegriffen werden muss, wird häufig auf die Dienste von darauf spezialisierten Unternehmen zurückgegriffen.

▶ Löschung bzw. Vernichtung von Datenträgern/Dokumenten

Die Löschung von magnetischen und optischen Datenträgern (z. B. Magnetbändern, Disketten, CDs, DVDs, Sticks) bzw. die Vernichtung von Datenträgern aller Art, insbesondere von nicht mehr benötigten Papierunterlagen, kann durch Dritte im Haus oder außer Haus erfolgen.

b) Privilegierung der Auftragsverarbeitung

Die Weitergabe von Daten des Verantwortlichen an einen Dienstleister ist im Fall der Auftragsverarbeitung gegenüber anderen Konstellationen der Datenweitergabe privilegiert. Bei Vorliegen der rechtlichen Voraussetzungen für eine Auftragsverarbeitung (insbesondere Art. 28 DSGVO) ist – von Sonderfällen (v. a. Drittlandfälle, siehe unten) abgesehen – für die Weitergabe personenbezogener Daten an den Auftragsverarbeiter sowie für die Verarbeitung durch diesen regelmäßig keine weitere Rechtsgrundlage im Sinne von Art. 6 bis 10 DSGVO erforderlich als diejenige, auf die der Verantwortliche selbst die Verarbeitung stützt.

Die Bedeutung dieses Privilegs ist erheblich. Grundsätzlich erfordert die Weitergabe von personenbezogenen Daten an eine externe Stelle eine gesonderte Rechtsgrundlage. Das kann – neben einer entsprechenden gesetzlichen Regelung – insbesondere die Einwilligung der betroffenen Person sein. Spezifische Rechtsgrundlagen zur Arbeitsteilung bei der Datenverarbeitung fehlen häufig. Da auch eine Einwilligung in die Datenweitergabe regelmäßig frei widerruflich ist, stellt diese keine verlässliche Basis für die angestrebte Arbeitsteilung dar. Das gilt umso mehr für die Datenverarbeitung durch Behörden, da die von der Datenschutz-Grundverordnung geforderte Freiwilligkeit einer Einwilligung der betroffenen Person (vgl. Art. 4 Nr. 11 DSGVO und Erwägungsgrund 43 DSGVO) oft zweifelhaft wäre.

Im Anwendungsbereich der Datenschutz-Richtlinie für Polizei und Strafjustiz ist die Freiwilligkeit einer Einwilligung der betroffenen Person in die Verarbeitung ihrer personenbezogenen Daten in besonderem Maße problematisch (vgl. Erwägungsgrund 35 Datenschutz-Richtlinie für Polizei und Strafjustiz). Sie ist als Rechtsgrundlage für eine Verarbeitung nicht vorgesehen (vgl. Art. 8 Abs. 1 Datenschutz-Richtlinie für Polizei und Strafjustiz).

Durch einen Vertrag zwischen Verantwortlichem und Auftragsverarbeiter, der die gesetzlichen Anforderungen erfüllt, kann jedoch eine rechtlich ausreichende Basis für die Weitergabe der Daten an einen Dienstleister geschaffen werden. In datenschutzrechtlicher Hinsicht gilt bei der Auftragsverarbeitung insoweit nichts anderes als beim Einsatz von eigenem Personal des Verantwortlichen; der Auftragsverarbeiter ist datenschutzrechtlich zwar Empfänger der Daten gemäß Art. 4 Nr. 9 DSGVO, jedoch kein „Dritter“ (vgl. Art. 4 Nr. 10 DSGVO). Stattdessen wird die Einheit der beiden Stellen fingiert.

c) Typische Vor- und Nachteile der Auftragsverarbeitung

Die Entscheidung, ob ein Dienstleister in die Erfüllung einer Verwaltungsaufgabe eingeschaltet werden soll, erfordert eine Abwägung, in die folgende typische Vor- und Nachteile einfließen können:

Vorteile der Auftragsverarbeitung können beispielsweise sein:

- Kosteneinsparung durch (vorübergehenden) Einsatz von externem Personal,
- Erhöhung der Planungssicherheit während der Dauer des Vertrages mit dem Dienstleister,
- Beseitigung historisch gewachsener Probleme durch Neukonzeption,

1. Allgemeines

- Unabhängigkeit von Hard- und Softwareaufrüstungen bzw. -wechseln,
- Unabhängigkeit von Personalqualifikationsproblemen und Personalengpässen,
- hohe Flexibilität,
- Konzentration des Personaleinsatzes auf die eigentlichen Kernaufgaben der öffentlichen Verwaltung,
- Steigerung der Qualität der Datenverarbeitung (Verbesserung von Arbeitsprozessen),
- effektiverer Datenschutz durch geschultes Personal und örtliche Gegebenheiten,
- Sicherstellung der Verfügbarkeit von Informationen und Diensten: 24 Stunden-Betrieb/365 Tage (Hochverfügbarkeit).

Demgegenüber drohen folgende Nachteile:

- Vertrauensverlust, wenn Dritte Zugang zu empfindlichen Bürger- oder Beschäftigtendaten erhalten,
- faktischer Herrschaftsverlust über die Verarbeitung der Daten,
- Haftungsrisiken, wenn sich der Auftragsverarbeiter nicht an die Vorgaben hält,
- Schadensrisiko (z. B. bei einer Löschung oder Beschädigung von Daten) aufgrund unsachgemäßer Datenverarbeitung durch einen (unzuverlässigen) Dienstleister,
- Kontrollverlust.

Jede Behörde muss sich fragen, ob es insbesondere aus Datenschutzgründen besser oder sogar notwendig ist, ihre Aufgaben durch eigene Kräfte zu erledigen. Hierbei sind auch rechtliche Erwägungen insbesondere zur Zulässigkeit der Auftragsverarbeitung in die Entscheidung einzubeziehen (zu Rechtsfragen ausführlich unter 2.).

Aus behördlicher Sicht ist vor allem zu bedenken, dass die Übertragung von Hilfstätigkeiten an einen externen Dienstleister eine mittelfristig nur schwer widerrufbare Entscheidung bedeuten kann. Nach Aufgabe des eigenen IT-Know-Hows kann es schwierig bis fast unmöglich sein, entsprechende Handlungsressourcen kurzfristig wieder aufzubauen. Dies gilt auch für das zur Überwachung und zur Kontrolle des Auftragsverarbeiters nötige Fachwissen. Der Behörde droht der Verlust von technischen Kernkompetenzen im Umgang mit den ihr anvertrauten Daten.

Auch wirtschaftliche Aspekte sind zu berücksichtigen. Schnell kann der Zustand eintreten, dass die Erreichung der etwa mit Outsourcing angestrebten Ziele (v. a. Einsparung von Ressourcen) aufgrund der zu ergreifenden Datenschutz- und Datensicherungsmaßnahmen in Frage gestellt oder gar verfehlt wird.

Andererseits kann vor allem die Ausgliederung einfacher Hilfstätigkeiten den eigenen Personalaufwand angesichts knapper Personalausstattung erheblich reduzieren und dem eigenen Personal die Konzentration auf die eigentlichen Sachaufgaben ermöglichen.

c) Vor- und Nachteile

Schon diese wenigen strategischen Gesichtspunkte zeigen, dass es keine Pauschalantworten geben kann, ob die Möglichkeit einer Auftragsverarbeitung genutzt werden soll oder nicht. Als Faustregel kann gelten: Je einfacher und je weniger grundrechtsrelevant eine Tätigkeit ist, umso eher kommt eine Erledigung durch externe Dienstleister in Betracht. Umgekehrt gilt: Je sensibler die der Behörde anvertrauten Daten sind, etwa im Steuer- oder Sozialrecht, umso eher muss die Behörde ihre Aufgaben in vollem Umfang selbst erfüllen und umso sorgfältiger muss sie vertragliche Vorkehrungen zur Risikominimierung treffen, wenn sie sich dennoch für eine Auftragsverarbeitung entscheidet.

2. Rechtliche Hinweise

Vor der Geltung der Datenschutz-Grundverordnung unterlag die Auftragsverarbeitung in den Mitgliedstaaten der EU noch jeweils eigenen Regeln. Diese Regeln – in Bayern insbesondere Art. 6 Bayerisches Datenschutzgesetz in der bis zum 24. Mai 2018 geltenden Fassung (BayDSG-alt) – wurden mit der Datenschutzreform 2018 im Grundsatz durch Art. 28 f. DSGVO ersetzt. Ziel der Neuregelung ist ein einheitlicher europäischer Datenschutzstandard mit unionsweit gleichen Pflichten und Zuständigkeiten. Auf Grundlage sogenannter „Öffnungsklauseln" kann der nationale Gesetzgeber jedoch noch ergänzende Bestimmungen treffen (vgl. ausführlich unten 2. b).

Nach dem bisherigen Recht geschlossene Verträge unterliegen keinem Bestandsschutz und müssen gegebenenfalls im jeweils erforderlichen Umfang an die Neuregelung angepasst werden. Sofern die Verträge die bisherigen rechtlichen Vorgaben beachten, dürfte der Anpassungsbedarf an die Datenschutz-Grundverordnung in der Regel aber überschaubar sein (zum künftig notwendigen Vertragsinhalt siehe unten 2. d und e). Angepasst werden sollten zudem die in zahlreichen Musterverträgen noch enthaltenen Verweise auf Vorschriften des früheren Rechts.

Vergleichender Überblick über ausgewählte Elemente der Neuregelung zur Auftragsverarbeitung

	Neues Recht (Art. 28 DSGVO)	Früheres Recht (Art. 6 BayDSG-alt)
Begriffe	Verantwortlicher – Auftragsverarbeiter	Auftraggeber – Auftragnehmer
Auswahl des Dienstleisters	Auftragsverarbeiter muss hinreichende Garantien im Hinblick auf geeignete technische und organisatorische Maßnahmen bieten	sorgfältig und unter besonderer Berücksichtigung der technischen und organisatorischen Maßnahmen
Möglicher Ort der Datenverarbeitung)	grundsätzlich weltweit	grundsätzlich EU/EWR
Haftung gegenüber betroffenen Personen bei Datenschutzverstößen	Verantwortlicher, Auftragsverarbeiter	grundsätzlich Auftraggeber
Dokumentationspflichten	Verantwortlicher, Auftragsverarbeiter	Auftraggeber
Hinweispflicht bei rechtswidrigen Weisungen	gesetzliche Pflicht	häufiger Vertragsinhalt

a) Beteiligte der Auftragsverarbeitung

Beteiligte der Auftragsverarbeitung sind der „Verantwortliche“ (aa) und der „Auftragsverarbeiter“ (bb). Die Abgrenzung der beiden Rollen kann mitunter Schwierigkeiten bereiten (cc).

aa) Verantwortlicher

Der Begriff des Verantwortlichen dient dazu, die Zuständigkeit für die Einhaltung datenschutzrechtlicher Anforderungen bei der Verarbeitung von personenbezogenen Daten zuzuweisen.

Verantwortlicher im Sinne der Datenschutz-Grundverordnung ist eine 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 (Art. 4 Nr. 7 DSGVO). Im Anwendungsbereich des neuen Bayerischen Datenschutzgesetzes konkretisiert Art. 3 Abs. 2 BayDSG dies dahingehend, dass – vorbehaltlich anderweitiger Bestimmungen – die für die (jeweilige) Verarbeitung zuständige öffentliche Stelle Verantwortlicher ist.

Nach Art. 5 Abs. 2 DSGVO muss der Verantwortliche die Rechtmäßigkeit der Datenverarbeitung auch nachweisen können (diese allgemeine „Rechenschaftspflicht“ wird an zahlreichen Stellen konkretisiert, z. B. in Art 7 Abs. 1, Art. 11 Abs. 2, Art. 12 Abs. 2 und Art. 24 Abs. 1 DSGVO). Diese Verantwortlichkeit besteht sowohl gegenüber der Aufsichtsbehörde als auch gegenüber den betroffenen Personen.

Die Einschaltung eines Auftragsverarbeiters wirkt sich auf die Verantwortlichkeit grundsätzlich nicht aus. Der Verantwortliche kann sich seinen datenschutzrechtlichen Pflichten und Verantwortlichkeiten nicht durch die Auslagerung seiner Datenverarbeitung entziehen. Er bleibt vielmehr auch im Fall der Auftragsverarbeitung Adressat der datenschutzrechtlichen Betroffenenrechte (z. B. bezüglich Auskunft bzw. Berichtigung oder Löschung) und hat dafür zu sorgen, dass die betroffenen Personen ihre Rechte tatsächlich wahrnehmen können (vgl. Art. 12 ff. DSGVO). Hierbei wird er jedoch nach Möglichkeit vom Auftragsverarbeiter unterstützt (Art. 28 Abs. 3 Buchst. e DSGVO).

Im Anwendungsbereich der Datenschutz-Richtlinie für Polizei und Strafjustiz sind die Art. 12 ff. DSGVO nicht anwendbar, die Betroffenenrechte ergeben sich aus den jeweiligen Spezialvorschriften.

bb) Auftragsverarbeiter

Auftragsverarbeiter ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet (Art. 4 Nr. 8 DSGVO). Gemäß Art. 29 DSGVO darf der Auftragsverarbeiter Daten ausschließlich auf Weisung des Verantwortlichen verarbeiten, es sei denn, er ist nach dem Unions- oder nationalen Recht zur Verarbeitung verpflichtet (z. B. gesetzliche Meldepflichten).

Der Auftragsverarbeiter darf die erhaltenen Daten nicht zu eigenen Zwecken nutzen und muss sich an die Weisungen des Verantwortlichen halten. Er wird weder „Herr der Daten“

noch selbst Verantwortlicher, sondern lediglich dessen „verlängerter Arm“. Er erhält keine Entscheidungsbefugnis bezüglich des Zwecks oder der wesentlichen Mittel der Datenverarbeitung. Es kommt auch nicht zu einer Übertragung behördlicher Zuständigkeiten auf ihn.

Die Datenschutz-Grundverordnung adressiert manche Pflichten, die den Verantwortlichen treffen, teils modifiziert auch an den Auftragsverarbeiter. Dazu zählen etwa Art. 30 DSGVO (Führung eines Verzeichnisses von Verarbeitungstätigkeiten), Art. 31 DSGVO (Zusammenarbeit mit der Aufsichtsbehörde), Art. 32 DSGVO (Sicherheit der Verarbeitung) und Art. 37 DSGVO (Bestellung eines Datenschutzbeauftragten).

cc) Abgrenzung von Verantwortlichem und Auftragsverarbeiter

Wenngleich der Auftragsverarbeiter vom Verantwortlichen im Grundsatz klar zu trennen ist, können sich in Grenzfällen durchaus schwierige Abgrenzungsfragen stellen.

Mit der umfassenden Weisungsgebundenheit (Art. 28 Abs. 3 Satz 1 und Satz 2 Buchst. a, Art. 29 DSGVO) ist es nicht vereinbar, dass ein Dienstleister – über die eigentliche Dienstleistung hinaus – eigene Interessen an den personenbezogenen Daten verfolgt. Wer selbst (auch) über den Zweck und über wesentliche Aspekte der Mittel der Datenverarbeitung bestimmt, ist in Bezug auf die Datenverarbeitung nicht ein dem Verantwortlichen untergeordneter Auftragsverarbeiter. Das betrifft insbesondere den Fall einer rechtswidrigen Überschreitung der Weisungen des Verantwortlichen durch den Auftragsverarbeiter. In Bezug auf eine solche Verarbeitung gilt der Auftragsverarbeiter selbst als Verantwortlicher (vgl. Art. 28 Abs. 10 DSGVO) mit den daraus folgenden Verpflichtungen.

Auch wer gemeinsam mit dem Verantwortlichen über Zwecke und Mittel der Verarbeitung personenbezogener Daten bestimmt, ist nicht Auftragsverarbeiter. Gemäß Art. 26 Abs. 1 DSGVO ist er neben dem (gegebenenfalls Haupt-) Verantwortlichen (weiterer) Verantwortlicher („gemeinsam Verantwortliche“). Ein Beispiel ist die Zusammenarbeit in Netzwerken. Gemeinsam Verantwortliche müssen in einer Vereinbarung in transparenter Weise festlegen, wer von ihnen welche datenschutzrechtlichen Pflichten erfüllt (Art. 26 Abs. 1 Satz 2 DSGVO).

Im Anwendungsbereich der Datenschutz-Richtlinie für Polizei und Strafjustiz sind bei gemeinsamer Verantwortlichkeit außerdem Art. 28 Abs. 2 Satz 2, Art. 30 BayDSG zu beachten.

dd) Kriterien zur Abgrenzung von Verantwortlichem und Auftragsverarbeiter

Für eine Auftragsverarbeitung spricht:

- Der Dienstleister besitzt keine Entscheidungsbefugnis hinsichtlich des Zwecks der Verarbeitung personenbezogener Daten; die öffentliche Stelle, die den Auftrag erteilt, behält die Hoheit über die Verwendung der Daten einschließlich deren Löschung oder Vernichtung.
- Der Dienstleister ist ausführlichen Weisungen der öffentlichen Stelle unterworfen, die ihm wenig Spielraum lassen.

- Die Daten werden dem Dienstleister von der öffentlichen Stelle lediglich zur Verfügung gestellt.
- Der Vertrag enthält Weisungen bezüglich der Art der durchzuführenden Datenverarbeitung und des Umgangs mit den personenbezogenen Daten (welche Daten wie lange zu welchem Zweck verarbeitet werden, wer Zugang zu ihnen hat), gewährt dem Dienstleister aber keine eigenen Nutzungsrechte. Es besteht somit ein vertragliches Nutzungsverbot.
- Der Dienstleister hat im Außenverhältnis (z. B. gegenüber Bürgern) keinerlei Entscheidungsbefugnisse.
- Der Dienstleister wird durch die öffentliche Stelle, die den Auftrag erteilt, überwacht.

Gegen eine Auftragsverarbeitung spricht:

- Der Dienstleister erhält das Recht zur Nutzung der personenbezogenen Daten zu eigenen Zwecken.
- Öffentliche Stelle und Dienstleister entscheiden gemeinsam über Zweck und wesentliche Elemente der Mittel der Datenverarbeitung.
- Die zugrunde liegende fachliche Aufgabe wird auf den Dienstleister übertragen.
- Die öffentliche Stelle besitzt keinen entscheidenden Einfluss auf die Datenverarbeitung durch den Dienstleister oder keine umfassenden Informationsrechte gegenüber dem Dienstleister.
- Der Dienstleister entscheidet auch selbst, auf welche Weise wann welche Daten verarbeitet werden.

b) Zulässigkeit der Auftragsverarbeitung

Art. 28 DSGVO enthält keine Beschränkung der Auftragsverarbeitung im Zusammenhang mit besonderen Rechtsgebieten. Grundsätzlich ist daher die Auftragsverarbeitung für alle Formen der Datenverarbeitung in allen Rechtsbereichen zulässig. Allerdings ist es dem nationalen Gesetzgeber auf Grundlage der sogenannten „Öffnungsklauseln“ der Datenschutz-Grundverordnung (hier: Art. 6 Abs. 3 und Abs. 2 DSGVO) möglich, spezifischere Bestimmungen zur Auftragsverarbeitung im öffentlichen Bereich zu treffen. Insbesondere in besonders sensiblen Bereichen kann hierdurch die Zulässigkeit der Auftragsverarbeitung eingeschränkt sein. Jede öffentliche Stelle, die den Einsatz eines Auftragsverarbeiters erwägt, sollte daher sorgfältig prüfen, ob bereichsspezifische Vorschriften besondere Voraussetzungen für eine Auftragsverarbeitung vorsehen oder diese insgesamt ausschließen.

Relevant ist das beispielsweise in folgenden Fällen:

- Verarbeitung von Meldedaten,
- Verarbeitung von Daten, die durch besondere Verschwiegenheitspflichten – wie Privat- oder Berufsgeheimnisse – geschützt sind (vgl. § 203 Strafgesetzbuch),

- Verarbeitung von Steuerdaten (vgl. § 30 Abgabenordnung),
- Verarbeitung von Sozialdaten (vgl. § 80 Zehntes Buch Sozialgesetzbuch),
- Verarbeitung von Patientendaten (vgl. Art. 27 Abs. 4 bis 6 Bayerisches Krankenhausgesetz) oder
- Verarbeitung von Personalaktendaten (Art. 108 Abs. 3 Bayerisches Beamtengesetz).

c) Auswahl des Auftragsverarbeiters

Der Auftragsverarbeiter muss nach den Vorgaben der Datenschutz-Grundverordnung, insbesondere im Hinblick auf Fachwissen, Zuverlässigkeit und Ressourcen, hinreichende Garantien dafür bieten, dass die Datenverarbeitung durch geeignete technische und organisatorische Maßnahmen im Einklang mit den rechtlichen Anforderungen erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet ist (Art. 28 Abs. 1 DSGVO und Erwägungsgrund 81 Satz 1 DSGVO). Der Verantwortliche muss den Auftragsverarbeiter anhand dieser Kriterien sorgfältig auswählen.

Dem Verantwortlichen selbst ist es häufig aber nicht möglich, die Einhaltung der datenschutzrechtlichen Anforderungen durch den Auftragsverarbeiter sicher zu beurteilen. Regelmäßig wird bei den technischen Kenntnissen und Fähigkeiten ein klares Gefälle zwischen dem Verantwortlichen und dem Auftragsverarbeiter bestehen. Grund für die Auftragsverarbeitung sind oft ja gerade die Spezialkenntnisse des externen Dienstleisters im Bereich der Datenverarbeitung.

Hier kommt vor allem Art. 28 Abs. 5 DSGVO dem Verantwortlichen entgegen. Befolgt der Auftragsverarbeiter genehmigte Verhaltensregeln (Art. 40 DSGVO) oder unterzieht er sich einem genehmigten Zertifizierungsverfahren (Art. 42 DSGVO), kann dies „als Faktor“ herangezogen werden, um die in Art. 28 Abs. 1 DSGVO geforderte Geeignetheit des Auftragsverarbeiters nachzuweisen (vgl. auch Erwägungsgrund 81 Satz 2 DSGVO).

Diese Vorschriften greifen nicht im Anwendungsbereich der Datenschutz-Richtlinie für Polizei und Strafjustiz, weshalb insoweit eine noch genauere Kontrolle des Auftragsverarbeiters erforderlich ist (vgl. Art. 28 Abs. 2 BayDSG).

Während die Auftragsverarbeitung innerhalb der EU bzw. des EWR den gleichen Regeln folgt, die auch bei der Beauftragung eines inländischen Dienstleisters gelten, sind bei einer Auftragsverarbeitung in einem Drittland zusätzlich die Art. 44 ff. DSGVO zu beachten. Art. 45 DSGVO regelt eine Datenübermittlung für die Fälle, in denen ein Angemessenheitsbeschluss der EU-Kommission vorliegt. Liegt ein solcher nicht vor, kommt eine Übermittlung von Daten auf Grundlage geeigneter Garantien gemäß Art. 46 DSGVO in Betracht, sofern den betroffenen Personen durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung stehen. Ansonsten kann ausnahmsweise eine Datenübermittlung unter den Bedingungen des Art. 49 DSGVO zulässig sein. Diese Regeln gelten auch bei der Übermittlung an eine internationale Organisation.

Insbesondere vor der Inanspruchnahme von Cloud-Leistungen ist daher genau zu prüfen, ob die Datenverarbeitung auch Datenübermittlungen in ein Drittland umfasst und die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.[2]

Diese Vorschriften greifen nicht im Anwendungsbereich der Datenschutz-Richtlinie für Polizei und Strafjustiz (vgl. Art. 28 Abs. 2 BayDSG), insoweit sind bereichsspezifische Sonderregelungen (z. B. Art. 58 des neuen Polizeiaufgabengesetzes – PAG) zu beachten.

Bei der Auswahl des Auftragsverarbeiters darf die Kostenfrage nicht die allein entscheidende Rolle spielen. In erster Linie muss derjenige Bewerber den Zuschlag bekommen, der das schlüssigste Datenschutz- und Datensicherheitskonzept vorweisen kann, und nicht derjenige, der zwar das günstigste Angebot abgibt, aber keine ausreichenden technischen und organisatorischen Sicherheitsmaßnahmen bietet. Auch das Vergaberecht verlangt nicht die Auswahl des billigsten, sondern des wirtschaftlichsten Angebots. Die Auswahl eines „geeigneten" Dienstleisters sollte ohnehin im eigenen Interesse erfolgen, denn jede Beeinträchtigung des Datenschutzes und der Datensicherheit durch den Dienstleister muss sich der Verantwortliche grundsätzlich zurechnen lassen, auch wenn er unter Umständen vom Dienstleister Ersatz für entstandene Schäden verlangen kann.

d) Vertrag zwischen Verantwortlichem und Auftragsverarbeiter

Die Auftragsverarbeitung beruht regelmäßig auf einem Vertrag zwischen dem Verantwortlichen und dem Auftragsverarbeiter. Der Vertrag ist schriftlich abzufassen. Das kann gemäß Art. 28 Abs. 9 DSGVO auch in einem elektronischen Format erfolgen. Besondere – insbesondere kommunalrechtliche – Formerfordernisse sind dabei zu beachten.

Nach Art. 28 Abs. 3 Satz 1 DSGVO kann eine Auftragsverarbeitung auch auf Grundlage eines „anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht der Mitgliedstaaten" erfolgen. Das Rechtsverhältnis zwischen dem Verantwortlichen und dem Auftragsverarbeiter muss in diesem Fall durch das „andere Rechtsinstrument" so geregelt werden, dass über die Rechte und Pflichten der beiden Beteiligten ebenso Klarheit besteht wie im Fall einer Auftragsverarbeitungsvereinbarung. Für Auftragsverarbeitungsverhältnisse insbesondere unter bayerischen öffentlichen Stellen hält das Landesrecht bislang keine „anderen Rechtsinstrumente" bereit. Mit ihrer Einführung, etwa durch eine entsprechende Rechtsverordnung, ist aber mittelfristig zu rechnen. Auf die „anderen Rechtsinstrumente" geht diese Orientierungshilfe gegenwärtig noch nicht ein.

Art. 28 Abs. 3 DSGVO bestimmt den Mindestinhalt, den der Vertrag über die Auftragsverarbeitung regeln muss. Erforderlich ist eine genaue Beschreibung der geschuldeten Tätigkeit des Dienstleisters. Die jeweilige Datenverarbeitung durch den Dienstleister muss immer einem konkreten Auftrag eines Verantwortlichen zugeordnet werden können.

[2] Vgl. hierzu ausführlich die Orientierungshilfe „Die Datenschutz-Grundverordnung und der internationale Datenverkehr", im Internet abrufbar unter https://www.datenschutz-bayern.de in der Rubrik „Datenschutzreform 2018 – Orientierungs- und Praxishilfen – Internationaler Datenverkehr".

Es müssen deshalb Gegenstand und Dauer sowie Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien der betroffenen Personen und die Rechte und Pflichten des Verantwortlichen vertraglich festgelegt sein. Im Einzelnen sind insbesondere folgende Punkte zu regeln:

- Der Beginn der Vertragslaufzeit ist eindeutig festzulegen. Ein Vertrag kann auch auf unbestimmte Dauer geschlossen werden. Es muss die Möglichkeit der Vertragsbeendigung bestehen.
- Die Modalitäten der Verarbeitung (vgl. Art. 4 Nr. 2 DSGVO: Erheben, Erfassen, Organisieren, Ordnen, Speichern, Übermitteln, Verändern und andere Vorgänge) müssen konkret und abschließend beschrieben werden.
- Der Verarbeiter darf keinen Spielraum hinsichtlich des Zwecks der Datenverarbeitung haben. Auf diese Weise wird die Zweckbindung der Daten auch bei der Auftragsverarbeitung sichergestellt.
- Es muss klar bestimmt sein, welche Arten personenbezogener Daten verarbeitet werden. Dies dient auch zur Bestimmung des erforderlichen Schutzniveaus, insbesondere bei der Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne von Art. 9 DSGVO (z. B. religiöse Überzeugungen, sexuelle Orientierung).

Zu den besonderen Anforderungen an die Verarbeitung von sensiblen Daten (Art. 9 Abs. 1 DSGVO) im Anwendungsbereich der Datenschutz-Richtlinie für Polizei und Strafjustiz vgl. auch Art. 29 Abs. 2 BayDSG. Zudem sind gegebenenfalls bereichsspezifische Sonderregelungen zu beachten, siehe etwa Art. 30 Abs. 2 PAG.

- Die Kategorien der betroffenen Personen (z. B. – je nach Verarbeitung – Kinder, Jugendliche, Beihilfeberechtigte, Beschäftigte, Lieferanten) müssen ebenfalls beschrieben werden. Auch dies kann sich auf das anzusetzende Datenschutzniveau auswirken.
- Die Rechte und Pflichten von Verantwortlichem und Auftragsverarbeiter sind festzulegen (dazu sogleich unter 2. e).

Im Anwendungsbereich der Datenschutz-Richtlinie für Polizei und Strafjustiz sind außerdem bei automatisierter Verarbeitung die Vorgaben der Art. 28 Abs. 2 Satz 2, Art. 32 Abs. 2 BayDSG zu beachten. Es sollte in einem Vertrag deshalb auch geregelt werden, wie diese Pflichten umgesetzt werden.

e) Rechte und Pflichten von Verantwortlichem und Auftragsverarbeiter

Im Vertrag über die Auftragsverarbeitung müssen die Rechte und Pflichten des Verantwortlichen und des Auftragsverarbeiters festgelegt werden.

Dabei können die Vertragspartner entscheiden, ob sie einen individuellen Vertrag formulieren oder – soweit verfügbar – auf ihre Situation passende Standardvertragsklauseln der Aufsichtsbehörden bzw. der EU-Kommission verwenden (vgl. Art. 28 Abs. 7 und 8 DSGVO).

e) Rechte und Pflichten

Standardvertragsklauseln sind als ein neues Instrument für weitgehend standardisierte Verfahren gedacht, die anerkannte Vertragsklauseln für einen ausgewogenen und datenschutzadäquaten Rahmen schaffen sollen. Es ist damit zu rechnen, dass im Laufe der Zeit verschiedene Standardvertragsklauseln verfügbar sein werden.

Der Vertrag muss nach Art. 28 Abs. 3 Satz 2 DSGVO mindestens Regelungen zu den folgenden Punkten vorsehen:

- **Weisungsgebundenheit (Art. 28 Abs. 3 Satz 2 Buchst. a DSGVO)**

  Der Auftragsverarbeiter verarbeitet die Daten nur auf dokumentierte Weisung des Verantwortlichen. Deshalb muss der Dienstleister auch auf die Erteilung von Weisungen des Verantwortlichen bestehen. Das gilt nur dann nicht, wenn der Auftragsverarbeiter durch das Recht der Union oder eines Mitgliedstaats ohnehin zur Verarbeitung der Daten verpflichtet ist; darauf muss er den Verantwortlichen grundsätzlich hinweisen.

- **Vertraulichkeit (Art. 28 Abs. 3 Satz 2 Buchst. b DSGVO)**

  Alle zur Datenverarbeitung eingesetzten Personen des Auftragsverarbeiters müssen zur Vertraulichkeit verpflichtet sein oder einer gesetzlichen Verschwiegenheitspflicht unterliegen. Der Auftragsverarbeiter muss die entsprechenden gesetzlichen oder sonstigen Verschwiegenheitsverpflichtungen des eingesetzten Personals jederzeit nachweisen können.

- **Technische und organisatorische Sicherungsmaßnahmen (Art. 28 Abs. 3 Satz 2 Buchst. c DSGVO)**

  Der Auftragsverarbeiter muss sich verpflichten, alle gemäß Art. 32 DSGVO erforderlichen Maßnahmen zu ergreifen.[3] Dazu zählen unter anderem:

  - Pseudonymisierung und Verschlüsselung personenbezogener Daten,
  - die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Datenverarbeitung auf Dauer sicherzustellen,
  - die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu diesen Daten nach einem Zwischenfall rasch wiederherzustellen, sowie
  - ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

  Das Ausmaß der Sicherungsmaßnahmen ist unter Berücksichtigung des Standes der Technik und der betroffenen Daten risikoangemessen zu bestimmen.[4]

[3] Diese Verpflichtung des Auftragsverarbeiters entbindet den Verantwortlichen freilich nicht von seinen Pflichten nach Art. 32 DSGVO, vgl. auch Art. 28 Abs. 3 Satz 2 Buchst. f DSGVO.

[4] Für die zu ergreifenden Maßnahmen siehe meinen Beitrag „Die Datenschutz-Grundverordnung (DSGVO) – Anforderungen an Technik und Sicherheit der Verarbeitung", im Internet abrufbar unter https://www.datenschutz-bayern.de in der Rubrik „Datenschutzreform 2018 – Informationsreihe – Einzelthemen", ferner die An-

Auch wenn nach dem Wortlaut des Art. 28 Abs. 3 Satz 2 Buchst. c DSGVO im Vertrag nur abstrakt die Einhaltung dieser Pflichten aus Art. 32 DSGVO aufgenommen werden muss, ist eine detaillierte Festschreibung der risikobasiert ausgewählten Maßnahmen – beispielsweise in Form einer Anlage zum Vertrag – schon aus Gründen der Rechenschaftspflicht, welcher der Verantwortliche unterliegt (vgl. Art. 5 Abs. 2, Art. 24 Abs. 1 Satz 1 DSGVO), in jedem Fall dringend empfehlenswert. Dazu zählen etwa auch Festlegungen in Bezug auf den Ort der Datenverarbeitung, den Zeitpunkt und die Art der Löschung bzw. Vernichtung von Datenträgern, die Versendungs- und Aufbewahrungsrichtlinien für Datenträger, die Eigentumsrechte an Hard- und Software, die System- und Benutzerdokumentation oder die Aufbewahrungspflichten. Gegebenenfalls kann diesbezüglich auf ein beim Auftragsverarbeiter vorhandenes Sicherheitskonzept Bezug genommen werden. Zudem ist ein Mechanismus vorzusehen, wonach der Verantwortliche über wesentliche Änderungen der technischen und organisatorischen Maßnahmen seitens des Auftragsverarbeiters zumindest informiert wird.

- **Unter-Auftragsverarbeiter (Art. 28 Abs. 3 Satz 2 Buchst. d DSGVO)**

Die Bedingungen für den Einsatz von „weiteren Auftragsverarbeitern“ (so bezeichnet die Datenschutz-Grundverordnung die bisher oft als „Unterauftragnehmer“ oder „Subunternehmer“ bezeichneten Stellen) müssen klar und in Einklang mit Art. 28 Abs. 2 und 4 DSGVO festgelegt sein. Dabei ist auch zu berücksichtigen, dass die Einbeziehung eines weiteren Auftragsverarbeiters (im Folgenden: Unter-Auftragsverarbeiter) stets der Genehmigung des Verantwortlichen bedarf. Hat der Verantwortliche zuvor eine diesbezügliche allgemeine Genehmigung erteilt, steht ihm gleichwohl ein Einspruchsrecht zu, wenn der Auftragsverarbeiter einen Unter-Auftragsverarbeiter hinzuziehen oder ersetzen möchte.

Damit der Verantwortliche seine Genehmigung erklären oder einen Unter-Auftragsverarbeiter ablehnen kann, muss der Auftragsverarbeiter den Verantwortlichen – auch im Fall einer zuvor erteilten allgemeinen schriftlichen Genehmigung – entsprechend informieren (vgl. Art. 28 Abs. 2 DSGVO). Für diese Information genügt es nicht, dem Verantwortlichen die bloße Möglichkeit einzuräumen, von entsprechenden Vorhaben Kenntnis zu nehmen. Unzureichend wäre beispielsweise, wenn der Auftragsverarbeiter beabsichtigte Hinzuziehungen oder Ersetzungen von Unter-Auftragsverarbeitern lediglich auf seiner Homepage veröffentlicht. Das gilt auch dann, wenn der Vertrag den Verantwortlichen verpflichten sollte, den Internet-Auftritt des Auftragsverarbeiters regelmäßig auf beabsichtigte Änderungen von Unter-Auftragsverarbeitungen zu überprüfen. Der Verantwortliche hat in diesem Zusammenhang keine „Holschuld“ hinsichtlich seiner Information. Art. 28 Abs. 2 DSGVO fordert vielmehr eine ausdrückliche, einzelfallbezogene Information des Auftragsverarbeiters gegenüber dem Verantwortlichen, die diesem auch tatsächlich die Entscheidung ermöglicht, die beabsichtigte Unter-Auftragsverarbeitung abzulehnen oder zu genehmigen.

Der Auftragsverarbeiter muss einem Unter-Auftragsverarbeiter dieselben Datenschutzpflichten auferlegen, die im Vertrag zwischen Verantwortlichen und Auftragsverarbeiter

forderungen zum IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik, im Internet abrufbar unter https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html.

festgelegt sind. Dabei muss auch der Unter-Auftragsverarbeiter hinreichende Garantien dafür bieten, dass die Datenverarbeitung durch geeignete technische und organisatorische Maßnahmen im Einklang mit den Anforderungen der Datenschutz-Grundverordnung erfolgt. Der Auftragsverarbeiter haftet grundsätzlich dem Verantwortlichen gegenüber für eine Verletzung von Datenschutzpflichten durch einen Unter-Auftragsverarbeiter (vgl. Art. 28 Abs. 4 DSGVO).

- **Unterstützung hinsichtlich der Betroffenenrechte (Art. 28 Abs. 3 Satz 2 Buchst. e DSGVO)**

  Der Auftragsverarbeiter muss den Verantwortlichen nach Möglichkeit mit technischen und organisatorischen Maßnahmen dabei unterstützen, dass dieser seinen Pflichten in Bezug auf die Rechte betroffener Personen (Art. 12 bis 22 DSGVO, z. B. Auskunfts- und Berichtigungsrechte) nachkommen kann. Ratsam ist eine möglichst konkrete Beschreibung der Unterstützungspflichten.

  

  Die Vorschriften der Art. 12 bis 22 DSGVO greifen nicht im Anwendungsbereich der Datenschutz-Richtlinie für Polizei und Strafjustiz (vgl. Art. 28 Abs. 2 BayDSG). Insoweit sind bereichsspezifische Sonderregelungen zu beachten.

- **Unterstützung hinsichtlich weiterer Pflichten des Verantwortlichen (Art. 28 Abs. 3 Satz 2 Buchst. f DSGVO)**

  Der Auftragsverarbeiter muss unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen bei der Erfüllung seiner Pflichten aus den Art. 32 bis 36 DSGVO unterstützen. Das betrifft

  - technische und organisatorische Sicherungsmaßnahmen des Verantwortlichen (Art. 32 DSGVO),
  - Meldungen von Datenschutzverletzungen an die Aufsichtsbehörde (Art. 33 DSGVO),
  - die Benachrichtigung der von Datenschutzverletzungen betroffenen Personen (Art. 34 DSGVO) und
  - die Durchführung von Datenschutz-Folgenabschätzungen und erforderlichenfalls die vorherige Konsultation der Datenschutz-Aufsichtsbehörde (Art. 35 und 36 DSGVO).

  

  Im Anwendungsbereich der Datenschutz-Richtlinie für Polizei und Strafjustiz gelten zum Teil erheblich abweichende Vorgaben:

  - Unanwendbarkeit von Art. 32 Abs. 3, 4 DSGVO, vgl. Art. 28 Abs. 2 Satz 2, Art. 32 Abs. 1 BayDSG,
  - besondere Anforderungen bei automatisierter Datenverarbeitung, vgl. Art. 32 Abs. 2 BayDSG,
  - weitergehende Pflichten bei der Unterstützung zur Meldung von Datenschutzverletzungen gemäß Art. 28 Abs. 2 Satz 2, Art. 33 BayDSG (Nachberichtspflicht),

- Unanwendbarkeit der Regelungen zur Datenschutz-Folgenabschätzung, vgl. Art. 28 Abs. 2 BayDSG. Insoweit sind bereichsspezifische Sonderregelungen (z. B. Art. 64 Abs. 2 PAG) zu beachten.

▶ Lösch- und Rückgabepflicht (Art. 28 Abs. 3 Satz 2 Buchst. g DSGVO)

Nach Beendigung der Auftragsverarbeitung gibt der Auftragsverarbeiter nach Wahl des Verantwortlichen alle personenbezogenen Daten zurück oder löscht sie, es sei denn, er unterliegt gesetzlichen Speicherungspflichten.

▶ Nachweis- und Hinweispflicht, Überprüfungsrecht (Art. 28 Abs. 3 Satz 2 Buchst. h, Satz 3 DSGVO)

Der Auftragsverarbeiter hat dem Verantwortlichen alle erforderlichen Informationen zur Verfügung zu stellen, die der Verantwortliche zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten benötigt.

Der Auftragsverarbeiter muss ferner Überprüfungen ermöglichen und hierzu beitragen, die der Verantwortliche oder ein von diesem beauftragter Prüfer (z. B. ein Sachverständiger) durchführt. Dabei muss der Auftragsverarbeiter schon deshalb aktiv mitwirken, weil er regelmäßig den besten Überblick über die Einzelheiten der Datenverarbeitung hat, z. B. hinsichtlich der eingesetzten Personen und Programme. Die genaue vertragliche Ausgestaltung dieser Pflichten muss im Einzelfall risikoorientiert festgelegt werden.[5]

Darüber hinaus ist der Auftragsverarbeiter verpflichtet, den Verantwortlichen darauf hinzuweisen, wenn er eine Weisung für datenschutzwidrig hält (vgl. Art. 28 Abs. 3 Satz 3 DSGVO).

▶ Weitergehende Vereinbarungen

Neben diesem Mindestinhalt sollte der Vertrag weitere Vereinbarungen enthalten.

Es sollten Klauseln in den Vertrag aufgenommen werden, die den Schutz der im Auftrag des Verantwortlichen verarbeiteten personenbezogenen Daten vor Zugriffen Dritter (z. B. bezüglich Pfändung, Beschlagnahme, Zwangsvollstreckung oder Insolvenz des Auftragsverarbeiters) dokumentieren. Dem Auftragsverarbeiter ist die Pflicht aufzuerlegen, in einem derartigen Falle den Verantwortlichen unverzüglich in Kenntnis zu setzen.

Zurückbehaltungsrechte aller Art (z. B. § 273 Bürgerliches Gesetzbuch oder § 369 Handelsgesetzbuch) sind hinsichtlich der verarbeiteten Daten und der dazugehörigen Datenträger ebenfalls vertraglich auszuschließen.

Der Auftragsverarbeitungsvertrag sollte auch Auskunft darüber geben, ob und in welcher Höhe Vertragsstrafen bezüglich Vertragsverletzungen vereinbart wurden. Ebenso sind Regelungen über eine vorzeitige Vertragskündigung bei schwerwiegenden Verstößen und eventuelle Schadensersatzansprüche in den Vertrag aufzunehmen.

[5] Zu den Kontrollen durch den Verantwortlichen siehe auch unten 2. f).

f) Überprüfung des Auftragsverarbeiters durch den Verantwortlichen

Aus der Verantwortlichkeit für die Einhaltung der datenschutzrechtlichen Anforderungen ergibt sich die Pflicht des Verantwortlichen, den Auftragsverarbeiter im erforderlichen Umfang zu überprüfen. Er muss sich grundsätzlich fortlaufend von der Einhaltung der zugesagten technischen und organisatorischen Maßnahmen durch den Auftragsverarbeiter überzeugen. Dementsprechend muss der Auftragsverarbeiter Überprüfungen ermöglichen und dazu beitragen (Art. 28 Abs. 3 Satz 2 Buchst. h DSGVO). Diese gesetzlich vorgeschriebene Mitwirkungspflicht darf grundsätzlich nicht von einem gesonderten Entgelt abhängig gemacht werden.[6]

Der Verantwortliche muss sich aber nicht zwingend selbst durch Vor-Ort-Kontrollen von der Einhaltung der datenschutzrechtlichen Anforderungen überzeugen. Große Bedeutung kann hier einem schlüssigen Datensicherheitskonzept des Auftragsverarbeiters zukommen, das der Verantwortliche selbst durch eigenes Personal oder mithilfe eines Sachverständigen überprüfen kann. Dabei gilt: Je sensibler die verarbeiteten Daten sind, desto umfangreicher müssen die Datensicherungsmaßnamen sein. Stellt sich im Rahmen der Kontrolle heraus, dass das festgelegte Sicherheitsniveau nicht ausreichend ist, sind ergänzende Maßnahmen zu vereinbaren, deren Umsetzung wiederum überwacht werden muss.

Eine Vor-Ort-Prüfung kann bei konkreten Anlässen bzw. Anhaltspunkten für ein Fehlverhalten des Dienstleisters geboten sein. Deshalb muss der Verantwortliche sich vertraglich ein Recht zu Vor-Ort-Kontrollen einschließlich entsprechender Betretungs- und Besichtigungsrechte einräumen lassen (Art. 28 Abs. 3 Satz 2 Buchst. h DSGVO).

g) Dokumentationspflichten

Sowohl der Verantwortliche als auch der Auftragsverarbeiter unterliegen gewissen Dokumentationspflichten.

- **Pflichten des Verantwortlichen**

  Art. 5 Abs. 2 DSGVO begründet für den Verantwortlichen eine allgemeine Rechenschaftspflicht: Der Verantwortliche muss nachweisen können, dass er die Verarbeitungsgrundsätze des Art. 5 Abs. 1 DSGVO einhält. Speziell mit Blick auf die Auftragsverarbeitung muss der Verantwortliche demnach insbesondere die Kriterien für die Auswahl des Auftragsverarbeiters, die Einhaltung der Vorgaben des Art. 32 DSGVO sowie die Durchführung und das Ergebnis einer Vor-Ort-Prüfung beim Auftragsverarbeiter dokumentieren. Darüber hinaus bestehen allgemeine Dokumentationspflichten, etwa hinsichtlich eines Verzeichnisses von Verarbeitungstätigkeiten (Art. 30 Abs. 1 DSGVO). Eine Ausnahme von den Dokumentationspflichten ist für öffentliche Stellen nicht vorgesehen.

[6] Vgl. hierzu ausführlich meine Aktuelle Kurz-Information 6, Keine gesonderte Entgeltpflicht für Kontrollen bei der Auftragsverarbeitung, im Internet abrufbar unter https://www.datenschutz-bayern.de in der Rubrik „Datenschutzreform 2018 – Aktuelle Kurz-Informationen".

2. Rechtliche Hinweise

▶ Pflichten des Auftragsverarbeiters

Auch der Auftragsverarbeiter unterliegt Dokumentationspflichten. Insbesondere muss er gemäß Art. 30 Abs. 2 DSGVO ein Verzeichnis zu allen Kategorien von im Auftrag eines Verantwortlichen durchgeführten Verarbeitungstätigkeiten führen, das folgende Angaben enthält:

- den Namen und die Kontaktdaten des Auftragsverarbeiters oder der Auftragsverarbeiter und jedes Verantwortlichen, in dessen Auftrag der Auftragsverarbeiter tätig ist, sowie gegebenenfalls des Vertreters des Verantwortlichen oder des Auftragsverarbeiters und eines etwaigen Datenschutzbeauftragten,
- die Kategorien von Verarbeitungen, die im Auftrag jedes Verantwortlichen durchgeführt werden,
- gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Art. 49 Abs. 1 UAbs. 2 DSGVO genannten Datenübermittlungen die Dokumentierung geeigneter Garantien sowie
- eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Art. 32 Abs. 1 DSGVO,

- im Anwendungsbereich der Datenschutz-Richtlinie für Polizei und Strafjustiz außerdem die Rechtsgrundlage der Verarbeitung sowie gegebenenfalls die Verwendung von Profiling (Art. 28 Abs. 2 Satz 2, Art. 31 BayDSG).

Das Verzeichnis von Verarbeitungstätigkeiten ist schriftlich zu führen, was auch „in einem elektronischen Format“ erfolgen kann (Art. 30 Abs. 3 DSGVO). Es muss der Aufsichtsbehörde auf Anfrage zur Verfügung gestellt werden (Art. 30 Abs. 4 DSGVO).

Darüber hinaus muss der Auftragsverarbeiter die Weisungen des Verantwortlichen dokumentieren (Art. 28 Abs. 3 Satz 2 Buchst. a DSGVO) und dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten zur Verfügung stellen (Art. 28 Abs. 3 Satz 2 Buchst. h DSGVO).

Nach Beendigung der Auftragsverarbeitung ist die Rückgabe bzw. Löschung der Daten gemäß Art. 28 Abs. 3 Satz 2 Buchst. g DSGVO zu dokumentieren. Mit Blick auf seine Pflicht zur Unterstützung des Verantwortlichen (Art. 28 Abs. 3 Satz 2 Buchst. h DSGVO) sollte der Auftragsverarbeiter auch Prozesse für die Durchsetzung der Betroffenenrechte (Art. 28 Abs. 3 Satz 2 Buchst. e DSGVO) und hinsichtlich der Melde- und gegebenenfalls Benachrichtigungspflicht bei Datenschutzverletzungen (Art. 33, 34 DSGVO) dokumentieren.

Im Anwendungsbereich der Datenschutz-Richtlinie für Polizei und Strafjustiz gilt dies auch für die Benachrichtigungspflicht gemäß Art. 33 BayDSG.

h) Haftungsfragen

Jeder an einer Verarbeitung beteiligte Verantwortliche haftet gemäß Art. 82 Abs. 2 Satz 1 DSGVO für den Schaden, der durch eine nicht der Datenschutz-Grundverordnung entsprechende Datenverarbeitung verursacht wurde. Dagegen haftet ein Auftragsverarbeiter nur, wenn er seinen speziellen Pflichten als Auftragsverarbeiter nicht nachgekommen ist. Dazu zählt vor allem die Nichtbeachtung der rechtmäßig erteilten Anweisungen des Verantwortlichen.

Sind mehrere Verantwortliche und/oder Auftragsverarbeiter für einen durch die Verarbeitung verursachten Schaden verantwortlich, so haften sie grundsätzlich gesamtschuldnerisch („jeder trägt alles"). Auf diese Weise soll ein wirksamer Schadensersatz für die betroffene Person sichergestellt werden (Art. 82 Abs. 4 DSGVO). Ein Verantwortlicher oder ein Auftragsverarbeiter wird von der Haftung befreit, wenn er nachweist, dass er in keiner Weise für den Schaden verantwortlich ist (Art. 82 Abs. 3 und Erwägungsgrund 146 Satz 2 DSGVO).

Jeder Verantwortliche oder Auftragsverarbeiter, der den vollen Schadenersatz geleistet hat, kann anschließend – gegebenenfalls anteilig – Rückgriff bei anderen an derselben Verarbeitung beteiligten Verantwortlichen oder Auftragsverarbeitern nehmen (Art. 82 Abs. 5 DSGVO).

Nach Erwägungsgrund 146 Satz 4 DSGVO bleiben weitergehende Schadensersatzansprüche auf der Grundlage von Unions- oder nationalem Recht unberührt.

Im Anwendungsbereich der Datenschutz-Richtlinie für Polizei und Strafjustiz sind diese Haftungsregeln nicht anwendbar. Hier gilt Art. 37 BayDSG. Unter den Voraussetzungen des Art. 37 Abs. 5 BayDSG sind auch andere, bereichsspezifische Sonderregelungen zu beachten.

3. Befugnisse der Aufsichtsbehörden

Art. 58 DSGVO räumt den Aufsichtsbehörden auch mit Blick auf die Auftragsverarbeitung weitreichende Untersuchungs- und Abhilfebefugnisse ein. So kann der Bayerische Landesbeauftragte für den Datenschutz im Rahmen seiner Zuständigkeit für bayerische öffentliche Stellen unter anderem

- den Verantwortlichen und den Auftragsverarbeiter anweisen, alle Informationen herauszugeben, die für die Erfüllung seiner Aufgaben erforderlich sind,
- Untersuchungen in Form von Datenschutzprüfungen vornehmen,
- vom Verantwortlichen und Auftragsverarbeiter Zugang zu allen für die Erfüllung der Aufgaben erforderlichen personenbezogenen Daten verlangen,
- Zugang zu den Geschäftsräumen fordern,
- die Datenverarbeitung vorübergehend oder endgültig beschränken oder untersagen,
- eine Zertifizierung widerrufen oder die Zertifizierungsstelle hierzu anzuweisen.

Im Anwendungsbereich der Datenschutz-Richtlinie für Polizei und Strafjustiz bestehen die in den letzten beiden Unterpunkten genannten Möglichkeiten nicht (vgl. Art. 28 Abs. 2 Satz 2, Art. 34 Abs. 1 Satz 1 BayDSG).

Den Aufsichtsbehörden steht damit ein wirksames Instrumentarium zur Durchsetzung der datenschutzrechtlichen Anforderungen zur Verfügung.

4. Nähere Erläuterungen zu einzelnen Formen der Auftragsverarbeitung

a) Vernichtung von Datenträgern

aa) Allgemeines

Eine betroffene Person hat regelmäßig ein Recht auf Löschung der sie betreffenden personenbezogenen Daten, wenn die Daten für die Zwecke, für die sie erhoben wurden, nicht mehr erforderlich sind. Das Löschen von Daten stellt gemäß Art. 4 Nr. 2 DSGVO eine Form der Verarbeitung dar.

Eine Löschung von Daten kann auch durch die Vernichtung der Datenträger erfolgen. Dabei ist zu beachten, dass die Anforderungen an technische und organisatorische Maßnahmen bei der Vernichtung von Datenträgern umso höher sein müssen, je höher die Sensibilität der Daten ist. Hierbei können die Festlegungen zur Informationsdatenträgervernichtung bei unterschiedlichen Sicherheitsstufen in der 2012 veröffentlichten DIN 66399 „Büro- und Datentechnik – Vernichtung von Datenträgern“ herangezogen werden.

bb) Vernichtung in Form einer Auftragsverarbeitung

Der Verantwortliche trägt auch dann die Verantwortung für die Einhaltung der Datenschutzvorschriften, wenn er einen Auftragsverarbeiter mit der Vernichtung von Datenträgern mit personenbezogenen Daten beauftragt (Art. 5 Abs. 2 DSGVO). Der Verantwortliche muss auch bei dieser Form der Auftragsverarbeitung den Dienstleister sorgfältig auswählen (vgl. bereits 2. c). Der Verantwortliche sollte sich deshalb bereits vor Vertragsunterzeichnung vor Ort davon überzeugen, dass der Dienstleister tatsächlich dazu in der Lage ist, die datenschutzgerechte Entsorgung sicherzustellen. Auch die ordnungsgemäße Durchführung der Vernichtung der Datenträger ist zumindest stichprobenartig zu überprüfen. Ein Recht auf unangemeldete Kontrollen bei der Entsorgung ist im Rahmen der Beauftragung des Entsorgungsunternehmens zu vereinbaren.

Ein Entsorgungskonzept darf sich aber nicht allein auf Maßnahmen zur Vernichtung der Datenträger beschränken, sondern muss auch die Sammlung und Lagerung (einschließlich einer etwaigen Zwischenlagerung), den Transport, die Organisation sowie die mit externen Entsorgungsunternehmen zu vereinbarenden vertraglichen Regelungen einbeziehen und damit den gesamten Entsorgungsvorgang und seine Vorphasen entsprechend berücksichtigen. Maßnahmen für den Fall menschlichen Versagens sind ebenso vorzusehen wie solche für den Fall von Funktionsstörungen technischer Systeme. Das Ziel muss sein, von der Sammlung des Vernichtungsgutes bis zur endgültigen Entsorgung ein gleichmäßig hohes Sicherheitsniveau zu erreichen, das der festgelegten Sicherheitsstufe entspricht.

Bei der Vernichtung von personenbezogenen Daten im Auftrag sind insbesondere folgende Punkte zu regeln (vgl. auch oben 2. d und e):

- Festlegung der Art und Menge der zu entsorgenden Datenträger und der dabei zu berücksichtigenden Schutzstufe,
- Auswahl eines geeigneten Vernichtungsverfahrens,
- Bestimmung des Ortes und des Zeitpunktes der Vernichtung (z. B. vor Ort beim Verantwortlichen oder in der Betriebsstätte des Auftragsverarbeiters) und der dabei zu ergreifenden Maßnahmen der Zugangskontrolle (z. B. Maßnahmen zur Gebäudesicherung),
- Festlegung der Verantwortlichkeiten für die Aufbewahrung und den Transport der Datenträger (eventuell durch Subunternehmer); Festlegung der dabei zu ergreifenden Maßnahmen der Transportkontrolle (z. B. Beschreibung von Transportwegen und Transportbehältnissen),
- Verpflichtung/Hinweis des Personals des Auftragsverarbeiters auf das Datengeheimnis,
- Gewährleistung durch den Auftragsverarbeiter, dass Unbefugte keine Kenntnis der auf den Datenträgern gespeicherten Daten erhalten können,
- Informationspflicht des Auftragsverarbeiters in bestimmten Ausnahmefällen (beispielsweise bei Betriebsstörungen, im Fehlerfalle, bei Verstößen),
- Haftungsregelung,
- Regelung von Unterauftragsverhältnissen,
- Berechtigung des Verantwortlichen zur Durchführung von Überprüfungen bei der Aufbewahrung, dem Transport und bei der Vernichtung der Datenträger sowie
- Festlegung von Art und Form der zu übergebenden Bescheinigungen bei Abholung bzw. nach ordnungsgemäßer Vernichtung durch den Auftragsverarbeiter bei jedem Entsorgungsvorgang.

cc) Zwischenlagerung des Entsorgungsgutes

Eine zusätzliche Schwachstelle stellt gelegentlich die ungesicherte Lagerung des Entsorgungsgutes bis zu seiner Abholung durch den Auftragsverarbeiter dar. Datenträger mit personenbezogenen Daten sind bis zu ihrer endgültigen Vernichtung unter Verschluss in abschließbaren Räumen oder Containern zu bewahren.

Im Anwendungsbereich der Datenschutz-Richtlinie für Polizei und Strafjustiz sind bei automatisierter Verarbeitung außerdem die Vorgaben des Art. 32 Abs. 2 BayDSG zu beachten.

b) (Fern-)Wartung

In Behörden und Kommunen wird heute eine Vielzahl spezieller Hard- und Software eingesetzt, deren alleinige Wartung durch das eigene Personal wegen der dafür benötigten Spe-

zialkenntnisse vielfach nicht mehr möglich ist, so dass bei Störungen oft der Hersteller oder ein externer Sachverständiger eingeschaltet werden muss. Das kann vor Ort geschehen, meist jedoch im Rahmen des Teleservice, also in Form einer Ferndiagnose und -wartung. Bei der Hardwarewartung wird in der Regel nur auf bestimmte Statusinformationen in eigens dafür eingerichteten Diagnosedateien zugegriffen, die keine personenbezogenen Daten enthalten. Bei vielen Datenverarbeitungssystemen kann aber die Fehlerdiagnose und -behebung mit einer Offenbarung geschützter personenbezogener Daten verbunden sein. Kann bei der Prüfung oder Wartung ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden, gelten die Regeln der Auftragsverarbeitung nach Art. 28 Abs. 1 bis 4, 9 und 10 DSGVO entsprechend (Art. 5 Abs. 3 Satz 1 BayDSG).

Dabei ist eine Fernwartung datenschutzrechtlich besonders problematisch. Bei einer Wartung vor Ort sind die Kontroll- und Eingriffsmöglichkeiten des eigenen Personals im Regelfall größer. Es ist dann eher erkennbar und prüfbar, welche konkreten Personen in Erscheinung treten; zudem ist ein „Entfernen", Verändern, unzulässiges Lesen oder Übertragen von Daten durch die Kontrolle erschwert.

Bei Einsatz einer Fernwartung ist daher insbesondere auf die Einhaltung folgender Regeln zu achten (vgl. auch oben 2. d und e):

- Der Verantwortliche definiert Art und Umfang der Fernwartung sowie die Abgrenzung der Kompetenzen und Pflichten zwischen Wartungs- und Kundenpersonal im Wartungsvertrag. Für Zuwiderhandlungen empfiehlt es sich, empfindliche Vertragsstrafen vorzusehen.
- Das Wartungspersonal muss auf das Datengeheimnis verpflichtet/hingewiesen sein.
- Eine Weitergabe der im Rahmen der Fernwartung anfallenden Daten ist zu untersagen.
- Für die Durchführung der Fernwartung muss eine eigene Benutzerkennung eingerichtet werden. Das dazugehörige Passwort ist nach jedem Wartungsvorgang zu ändern.
- Bei der Fernwartung ist die Verbindung oder die Freischaltung (nach einem Authentifikationsprozess) stets vom Verantwortlichen aus aufzubauen (z. B. mittels eines Call-Back-Verfahrens) oder freizugeben, damit sichergestellt ist, dass keine unbefugten Einwählversuche stattfinden können. Nach Abschluss der Wartungsarbeiten ist diese Verbindung wieder zu deaktivieren.
- Eine Benutzung des Internets für die Datenübertragung sollte nur dann erfolgen, wenn sowohl der Auftragsverarbeiter als auch der Verantwortliche durch geeignete Firewall-Systeme vom offenen Netz abgeschottet sind.
- Vom Verantwortlichen sind der Wartung/Fernwartung nur solche Zugriffsmöglichkeiten zu eröffnen, die für die Fehlerbehebung unbedingt erforderlich sind („Prinzip der geringsten Rechtevergabe"). Es ist ferner darauf zu achten, dass im Rahmen der Wartung bzw. Fernwartung, soweit möglich, keine Funktionen freigeschaltet werden, die eine Übertragung oder Auswertung von Datenbeständen des Verantwortlichen zulassen. Falls eine Übertragung personenbezogener Daten unbedingt erforderlich ist, dürfen die-

se Daten in der Fernwartungszentrale nur temporär gespeichert werden. Ein zweckwidriger Zugriff auf andere Rechner im Netz ist zu unterbinden.

- Soweit möglich, müssen alle Aktivitäten im Rahmen der Fernwartung vom Verantwortlichen online mitverfolgt werden. Im Zweifelsfalle muss dieser auch die Aktivitäten abbrechen können.
- Außerdem sind alle Aktivitäten der Fernwartung aufzuzeichnen und die entsprechenden Protokolle auszuwerten. Bei besonders kritischen Aktionen ist der gesamte Dialog zu protokollieren, damit später erkennbar wird, auf welche Daten zugegriffen wurde.
- Zur Sicherung der Vertraulichkeit der übertragenen Daten auf dem Übertragungswege kann es erforderlich sein, dass die Daten verschlüsselt werden. Es ist in diesem Falle jedoch darauf zu achten, dass die Protokollierung vor Ort unverschlüsselt erfolgt. Nur so ist eine effektive Kontrolle durch den Verantwortlichen gewährleistet.

Im Anwendungsbereich der Datenschutz-Richtlinie für Polizei und Strafjustiz sind bei automatisierter Verarbeitung außerdem die Vorgaben des Art. 32 Abs. 2 BayDSG zu beachten.

c) Outsourcing im klassischen Sinn

Eine pauschale Bewertung und Aussage, welche Datenschutz- und Datensicherungsmaßnahmen bei welchem Umfang von Outsourcing notwendig und angemessen sind, lässt sich selten treffen. Es ist stets eine Einzelfallprüfung erforderlich. Hinzu kommt, dass natürlich die Art der verarbeiteten Daten hinsichtlich ihrer besonderen Schutzbedürftigkeit berücksichtigt werden muss, so dass schon aus diesen Gründen das Outsourcing vielfach ausscheiden wird. Im Übrigen kann gerade in solchen Fällen sehr schnell der Zustand erreicht werden, dass die mit dem Outsourcing angestrebten Ziele (Kosteneinsparung) aufgrund der zu ergreifenden umfangreichen Datenschutz- und Datensicherungsmaßnahmen nur schwer oder gar nicht erreicht werden. Auch eine Wirtschaftlichkeitsbetrachtung der Outsourcing-Maßnahme unter Berücksichtigung des Aufwandes für die erforderlichen Sicherheitsmaßnahmen ist hier dringend zu empfehlen.

aa) Auslagerung der Systemadministration

Eine Übernahme der Systemadministration der Server und der Überwachung des lokalen Netzwerkes einer öffentlichen Stelle mittels Fernwartung durch eine andere damit beauftragte Stelle muss im Wesentlichen den Regeln der Auftragsverarbeitung entsprechen, wenn ein Zugriff des Dienstleisters auf personenbezogene Daten nicht ausgeschlossen werden kann (vgl. Art. 5 Abs. 3 Satz 1 BayDSG). Daher ist der Auftrag schriftlich zu erteilen, wobei u. a. die technischen und organisatorischen Maßnahmen festzulegen sind. Unbedingt erforderlich (vgl. auch oben 2. d und e) sind insbesondere Festlegungen betreffend:

- die Zugangskontrolle (z. B. Identifikation und Authentisierung, sicherer Verbindungsaufbau mittels eines Call Back-Verfahrens über eine Firewall, dezidierte Vergabe von Zugriffsrechten und Wartungsprivilegien, Protokollierung aller Zugriffe, Ergreifung von Maßnahmen beim unberechtigten Datenzugriff),

- die Wahrung der Vertraulichkeit (z. B. Einsatz von Datenverschlüsselungskomponenten bei der Datenspeicherung und der Datenübertragung, Errichtung von „Virtuellen Privaten Netzen“),
- Kontrollmaßnahmen des Verantwortlichen (z. B. Kontrolle der Wartungsaktivitäten online oder mittels ausgewerteter Wartungsprotokolle, gegebenenfalls Unterbrechungsmöglichkeit der Fernwartung) sowie
- organisatorische Maßnahmen des Auftragsverarbeiters (z. B. Einhaltung der Verschwiegenheitsvorschriften, schriftliche Festlegung der Wartungsaktivitäten, Kontrolle der Protokolle).

Bei einer Systemadministration durch den Dienstleister ist – anders als bei einer reinen Hard- bzw. Software-Fernwartung – neben einer Datenverschlüsselung – soweit möglich – insbesondere eine umfassende Protokollierung aller Systemaktivitäten vorzusehen. Aus den Protokollen muss sich die Frage beantworten lassen: „Wer hat wann mit welchen Mitteln was veranlasst bzw. worauf zugegriffen?“ Außerdem müssen sich Systemzustände ableiten lassen: „Wer hatte von wann bis wann welche Zugriffsrechte?“

Folgende Aktivitäten sind zur Überwachung der Systemadministrations- und Fernwartungsaktivitäten vollständig zu protokollieren:

- Systemgenerierung und Modifikation von Systemparametern,
- Einrichten von Benutzern,
- Verwaltung von Befugnistabellen,
- Änderungen an der Dateiorganisation,
- Durchführung von Backup-, Restore- und sonstigen Datensicherungsmaßnahmen,
- Aufruf von Administrations-Tools,
- Versuche des unbefugten Einloggens sowie der Überschreitung von Befugnissen,
- Datenübermittlungen,
- Benutzung von automatisierten Abrufverfahren,
- Eingabe, Veränderung und Löschung von Daten durch den Auftragsverarbeiter sowie
- Aufrufe von besonders „sensiblen“ Programmen.

Die Zwangsläufigkeit und damit die Vollständigkeit der Protokolle muss gewährleistet werden. Das Gleiche gilt für die Manipulationssicherheit der Einträge in den Protokolldateien. Die Protokolle müssen durch den Verantwortlichen ausgewertet werden können. Dazu sind sie so zu gestalten, dass eine effektive Überprüfung möglich ist.

Im Übrigen ist zu bedenken, dass bei einer Auslagerung von Systemadministrationstätigkeiten an eine andere Stelle die Aufrechterhaltung eines ordnungsgemäßen Betriebes der Datenverarbeitungsanlagen, z. B. im Falle eines Streiks beim Auftragsverarbeiter, nicht gewährleistet ist.

bb) Outsourcing (von Teilen) des Datenbestandes

Die Vorhaltung umfangreicher Bestände personenbezogener Daten von Behörden und Kommunen in einer Datenbank eines privaten Rechenzentrumsbetreibers im Rahmen der

4. Nähere Erläuterungen zu einzelnen Formen der Auftragsverarbeitung

Auftragsverarbeitung kann unter Beachtung der nachstehenden Ausnahmen zulässig sein. Sie ist allerdings nicht immer wünschenswert, da sich die Gefahr erhöht, dass Unberechtigte auf die den Gemeinden und Behörden großenteils nicht freiwillig anvertrauten Daten der Bürger Zugriff nehmen können.

Bei Datenbeständen, die in Form einer Auftragsverarbeitung ausgelagert werden dürfen, muss darauf geachtet werden, dass eine Kenntnisnahme und ein Zugriff insbesondere auf sensible Datenbestände durch den Dienstleister im Hinblick auf die schutzwürdigen Belange betroffener Personen, z. B. durch Verschlüsselung, auszuschließen ist.

Bei der Wahl der Verschlüsselung sind grundsätzlich die Empfehlungen des Bundesamts für Sicherheit in der Informationstechnik für kryptographische Verfahren[7] zu beachten. Außerdem ist zur Wahrung der Vertraulichkeit und Integrität der Daten eine Verschlüsselung der Daten auf dem Übertragungsweg zwingend erforderlich.

Zur Durchführung der Verschlüsselung bietet sich die Einrichtung eines virtuellen privaten Netzes (VPN) an. Ein VPN ist ein Netzwerk, welches von der öffentlichen Telekommunikationsstruktur Gebrauch macht, gleichzeitig aber die Privatsphäre durch den Einsatz von so genannten Tunneling- und Sicherheitsprotokollen schützt und in der Regel über das Internet realisiert wird.

Neben den allgemein bekannten Sicherheitsmaßnahmen (z. B. rigorose Beschränkung der Zugriffs- und Nutzungsrechte auf das unbedingt Notwendige, Ergreifung von Maßnahmen zur Virenbekämpfung, Auswertung von Sicherheitsverletzungen in den maschinell geführten Protokollen und effektiver Passwortschutz) müssen im Rahmen eines Outsourcings von Datenbeständen zur Absicherung der Daten des Verantwortlichen zusätzliche Maßnahmen ergriffen werden. So müssen beispielsweise alle Server durch Maßnahmen der Zugangskontrolle physisch geschützt werden. Die Datenzugriffe auf Server und insbesondere die Nutzung administrativer Berechtigungen müssen intensiv mit Hilfe der Protokollierung überwacht werden.

Natürlich ist es gerade bei dieser Form der Auftragsverarbeitung zwingend erforderlich, dass sich der Verantwortliche regelmäßig von der Gewährleistung der Datensicherheit durch den Auftragsverarbeiter überzeugt.

cc) Zentrale Datenbank verschiedener Verantwortlicher

Bei der Vorhaltung personenbezogener Daten verschiedener Verantwortlicher in einer zentralen Datenbank ist zusätzlich darauf zu achten, dass die Datenbestände zumindest logisch getrennt voneinander gespeichert werden. Bei einer zentralen Datenbank wiegt ein Missbrauch dieser Datenbank regelmäßig schwerer als bei der Datenbank eines einzelnen Verantwortlichen, da die zentrale Datenbank einen umfassenderen, vernetzbaren Datenbestand aufweist. Aus allgemeinen datenschutzrechtlichen Überlegungen heraus ist es zudem wünschenswert, zentrale Datensammlungen möglichst zu verhindern oder, soweit sie sich nicht

[7] Bundesamt für Sicherheit in der Informationstechnik, Technische Richtlinie Kryptographische Verfahren: Empfehlungen und Schlüssellängen (BSI TR-02102-1), im Internet abrufbar unter https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/index_htm.html.

vermeiden lassen, ihre Zahl möglichst gering zu halten, da sie eine erhöhte Gefahr in sich bergen, unzulässigerweise oder gegebenenfalls auch für andere Zwecke als den, zu dem sie angelegt wurden, genutzt zu werden.

Der Zugriff auf die Daten ist darüber hinaus insoweit zu beschränken, dass jeder Verantwortliche nur „seine eigenen" Daten abrufen kann. Daher muss sichergestellt sein, dass geeignete Vorkehrungen getroffen werden, um einen Zugriff unbefugter Dritter – und zwar auch von Verantwortlichen, welche gleiche Aufgaben mit anderer örtlicher Zuständigkeit wahrnehmen – auf die gespeicherten Daten zu verhindern.

dd) Backup-Service

Viele kleinere Behörden und Gemeinden sichern zwar täglich ihre Daten, prüfen jedoch nicht, ob diese Sicherungen vollständig und korrekt sind. Hinzu kommt, dass vielfach beim Anwender gar nicht das Know-How vorhanden ist, nach einem Systemzusammenbruch mit den Sicherungsbeständen einen Wiederanlauf erfolgreich durchzuführen.

So gibt es heute Anbieter, die die Sicherungsbestände unter Anwenderbedingungen auf ihre Verwendbarkeit hin testen. Eine solche Dienstleistung ist für viele Anwender wertvoll und unverzichtbar, wenn man bedenkt, dass wegen fehlerhafter Datensicherungen Datenverluste auftreten können. Das kann im ungünstigsten Fall sogar dazu führen, dass die Datenbestände unter Umständen überhaupt nicht mehr rekonstruierbar sind. Aus diesem Grunde sollten zumindest die halb- oder vierteljährlich gezogenen Datensicherungen auf ihre Verwendbarkeit hin überprüft und als „Katastrophensicherungen" bis zur nächsten getesteten Vollsicherung unbedingt aufbewahrt werden.

Einige Hersteller von Standardanwendungssystemen bieten ihren Kunden einen so genannten Backup-Service an. Gerade kleinere Anwender sind häufig nicht dazu in der Lage, selbst entsprechend qualifizierte Mitarbeiter zu beschäftigen. Da aber auch diese Anwender in einem immer größer werdenden Maße von der Verfügbarkeit ihrer Datenverarbeitungsanwendungen abhängig sind, sollten sie diesen Service nutzen, ihre täglich gezogene Datensicherung bei Experten auf ihre Brauchbarkeit hin untersuchen zu lassen. Auf diese Weise kann frühzeitig – also bereits vor dem Eintritt eines Katastrophenfalls – auf Fehler und Unstimmigkeiten in der Datensicherung reagiert werden.

Natürlich müssen auch bei dieser Art von Auftragsverarbeitung der Datenschutz und die Datensicherheit gewährleistet sein. Die Überprüfung der Backup-Datenträger sollte daher möglichst in den Räumen des Verantwortlichen und unter Aufsicht seines Personals stattfinden. Dabei ist darauf zu achten, dass der Auftragsverarbeiter keine Kopien der Datenbänder erstellt, die er außer Haus schafft.

Im Anwendungsbereich der Datenschutz-Richtlinie für Polizei und Strafjustiz sind bei automatisierter Verarbeitung außerdem die Vorgaben des Art. 32 Abs. 2 BayDSG zu beachten.

d) Programmerstellung (auch Apps)

Soweit der Dienstleister mit dem Erstellen von Programmen beauftragt wurde, sollte darauf geachtet werden, dass dem Dienstleister keine Echtdaten, insbesondere keine personenbezogenen Daten zur Verfügung gestellt werden, auch nicht für Testzwecke. Da dem Verantwortlichen in der Regel im Rahmen der Softwareüberlassung nicht der so genannte Quellcode (Programmlogik), sondern lediglich der maschinell erzeugte Objektcode überlassen wird, muss er sich Gedanken darüber machen, wie er im Notfall trotzdem Zugriff auf den Quellcode erhält. Dies bedeutet, dass die Programmlogik bei einer vertrauenswürdigen Person oder Instanz hinterlegt werden muss, die in vertraglich festgelegten Fällen den Zugriff gestattet.

5. Checkliste

Die nachfolgende Checkliste soll die Prüfung unterstützen, ob wesentliche Inhalte in den Vertrag zur Auftragsverarbeitung einbezogen wurden. Angesichts der Vielgestaltigkeit der denkbaren Auftragsverarbeitungen und weil sich die konkrete Vertragsgestaltung auch nach der Schwere des Risikos für die Rechte und Freiheiten der betroffenen Personen richten muss, zielt die Checkliste nicht darauf ab, sämtliche Zweifelsfragen verbindlich zu klären. Sofern eine Frage mit „nein“ beantwortet wird, muss der Vertrag jedenfalls - auch anhand der vorangegangenen Ausführungen - auf seine rechtliche Zulässigkeit geprüft werden.

Die Checkliste konzentriert sich auf die datenschutzrechtlichen Fragestellungen und erhebt trotz ihres Umfangs keinen Anspruch auf Vollständigkeit.

Insbesondere bei von Auftragsverabeitern vorgelegten Verträgen ist zu prüfen, ob Vertragsinhalte missverständlich oder unklar sind, den sonstigen Vereinbarungen zwischen den Parteien oder gesetzlichen Vorgaben widersprechen.

Auf meiner Homepage https://www.datenschutz-bayern.de ist in der Rubrik „Datenschutzreform 2018 – Orientierungs- und Praxishilfen – Auftragsverarbeitung“ ein Mustervertrag zur Auftragsverarbeitung verlinkt, der die typischerweise wesentlichen Vertragsinhalte berücksichtigt. Dieser Mustervertrag wurde vom Bayerischen Staatsministerium des Innern, für Sport und Integration unter meiner Beteiligung erstellt.

Die Checkliste kann als Orientierungshilfe auch im Anwendungsbereich der Datenschutz-Richtlinie für Polizei und Strafjustiz verwendet werden; allerdings sind die bereichsspezifischen Besonderheiten zu beachten.

Checkliste Auftragsverarbeitung

Frage	Ja	Nein	Anmerkungen
Erfolgte eine sorgfältige Auswahl des Auftragsverarbeiters? Bietet der Auftragsverarbeiter hinreichende Garantien dafür, dass die Datenverarbeitung durch geeignete technische und organisatorische Maßnahmen im Einklang mit den datenschutzrechtlichen Anforderungen erfolgt?	☐	☐	
Liegen entsprechende Referenzen und/oder Zertifikate vor?	☐	☐	
Wird der Vertrag schriftlich bzw. in einem elektronischen Format geschlossen?	☐	☐	
Bleibt die Verantwortung für die ausgelagerten Bereiche bzw. Tätigkeiten beim Verantwortlichen?	☐	☐	
Enthält der Vertrag genaue Bestimmungen zu			
• Gegenstand der Verarbeitung?	☐	☐	
• Dauer der Verarbeitung?	☐	☐	
• Art der Verarbeitung?	☐	☐	
• Zweck der Verarbeitung?	☐	☐	
• Art der personenbezogenen Daten?	☐	☐	
• Kategorien der betroffenen Personen?	☐	☐	
• Rechten und Pflichten des Verantwortlichen?	☐	☐	
Hat der Auftragsverarbeiter die Weisungsgebundenheit versichert?	☐	☐	
Hat der Auftragsverarbeiter zugesagt, die Weisungen des Verantwortlichen zu dokumentieren?	☐	☐	
Dürfen die im Rahmen der Auftragsverarbeitung verarbeiteten Daten ausschließlich zur Erfüllung der vertraglich vereinbarten Leistung verwendet werden (Gebot der Zweckbindung)?	☐	☐	
Wurden dem Auftragsverarbeiter Bekanntgabe, Verkauf, Vermietung oder anderweitige Verwendung der Daten durch Dritte bzw. die kommerzielle Verwendung verboten?	☐	☐	
Ist gewährleistet, dass sich die zur Verarbeitung befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen?	☐	☐	
Wurden diese Personen auf das Datengeheimnis verpflichtet bzw. hingewiesen?	☐	☐	
Hat sich der Verantwortliche davon durch eine Einsicht in die Verpflichtungs-/Hinweiserklärungen überzeugt?	☐	☐	
Wurden die Mitarbeiter des Auftragsverarbeiters bezüglich der Einhaltung des Datenschutzes und der Datensicherheit informiert und geschult?	☐	☐	
Werden im Rahmen der Auftragsverarbeitung ausschließlich fachlich geeignete Mitarbeiter eingesetzt?	☐	☐	

Checkliste Auftragsverarbeitung

Frage	Ja	Nein	Anmerkungen
Wurde beim Auftragsverarbeiter ein betrieblicher/behördlicher Datenschutzbeauftragter bestellt?	☐	☐	
Sind dessen Kontaktdaten bekannt?	☐	☐	
Wurden sowohl von Seiten des Verantwortlichen als auch des Auftragsverarbeiters verantwortliche Ansprechpartner zur Klärung eventuell auftretender fachlicher, technischer und organisatorischer Fragen benannt?	☐	☐	
Ist die Sicherheit der Datenverarbeitung angemessen gewährleistet (vgl. Art. 32 DSGVO), insbesondere mit Blick auf			
• Pseudonymisierung und Verschlüsselung?	☐	☐	
• Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste?	☐	☐	
• Datenverfügbarkeit und Wiederherstellbarkeit?	☐	☐	
• regelmäßige Überprüfung, Bewertung und Evaluierung der Sicherheitsmaßnahmen?	☐	☐	
Wurden detaillierte Sicherheitsanforderungen erarbeitet?	☐	☐	
Wurde daraufhin vom Auftragsverarbeiter ein entsprechendes Sicherheitskonzept entworfen und umgesetzt?	☐	☐	
Entspricht das Sicherheitskonzept den Anforderungen der Art. 32 ff. DSGVO?	☐	☐	
Wurde der Verantwortliche bei der Erstellung des Sicherheitskonzeptes einbezogen?	☐	☐	
Wurden sowohl die Vorgehensweise bei Sicherheitsverletzungen als auch das Eskalationsverfahren gemeinsam festgelegt?	☐	☐	
Werden revisionsfähige Aufzeichnungen über alle die Informationssicherheit betreffenden Vorkommnisse (z. B. Zugriffsverletzungen, Manipulationen, Hacking) geführt?	☐	☐	
Erfolgt eine regelmäßige Auswertung dieser Sicherheitsverletzungen?	☐	☐	
Wird dieses Sicherheitskonzept regelmäßig hinsichtlich seiner Gültigkeit überprüft und gegebenenfalls neuen Sicherheitsanforderungen angepasst?	☐	☐	
Liegt dieses Sicherheitskonzept dem Verantwortlichen in schriftlicher Form vor?	☐	☐	
Wurde dieses Sicherheitskonzept vom Verantwortlichen überprüft?	☐	☐	
Sind die Übermittlung bzw. Weitergabe von Daten und der Transport von Datenträgern vertraglich geregelt?	☐	☐	
Ist die Auslagerung von personenbezogenen Daten bzw. die Verschiebung von Dienstleistungen in das Ausland geregelt bzw. verboten?	☐	☐	
Ist eine Pflicht des Auftragsverarbeiters vereinbart, dem Verantwortlichen die Einhaltung der datenschutzrechtlichen Anforderungen nachzuweisen und Überprüfungen zu ermöglichen?	☐	☐	

Frage	Ja	Nein	Anmerkungen
Hängt die Vergabe von Unteraufträgen von der Genehmigung des Verantwortlichen ab bzw. kann er der Vergabe widersprechen?	☐	☐	
Unterliegt ein Unter-Auftragsverarbeiter den gleichen datenschutzrechtlichen Anforderungen wie der Auftragsverarbeiter?	☐	☐	
Ist eine Pflicht des Auftragsverarbeiters zur Unterstützung des Verantwortlichen hinsichtlich der Betroffenenrechte vereinbart?	☐	☐	
Ist der Auftragsverarbeiter vertraglich verpflichtet, den Verantwortlichen bei Einhaltung seiner Pflichten aus Art. 32 bis 36 DSGVO zu unterstützen?	☐	☐	
Ist eine Pflicht zur Löschung bzw. Rückgabe der Daten nach Beendigung des Auftrags vereinbart?	☐	☐	
Sind Zurückbehaltungsrechte hinsichtlich der Daten und Datenträger ausgeschlossen?	☐	☐	
Sind die Daten vor dem Zugriff Dritter sicher (z. B. Pfändung, Beschlagnahme)?	☐	☐	
Kann die Aufgabenerfüllung seitens des Verantwortlichen auch im Falle eines (vorzeitigen) Vertragsendes, eines Vertragsbruches, der Geschäftsaufgabe, der Insolvenz des Auftragsverarbeiters usw. sichergestellt werden?	☐	☐	
Sind Beginn, Mindestdauer und Ende des Vertrages eindeutig geregelt?	☐	☐	
Kann der Vertrag (unter Einhaltung einer entsprechenden Kündigungsfrist) beendet werden?	☐	☐	
Kann eine Vertragsauflösung bei krassen Vertragsverletzungen (z. B. bei groben Verletzungen von Geheimhaltungs- und Sicherheitsanforderungen) erfolgen?	☐	☐	
Wurden der Auftragsverarbeiter und das von ihm beschäftigte Personal dazu verpflichtet, alle im Rahmen der Auftragsverarbeitung erworbenen Kenntnisse und Informationen über den Verantwortlichen und die in seinem Auftrag verarbeiteten Daten auch nach der Vertragsauflösung vertraulich zu behandeln?	☐	☐	
Ist geregelt, welches Gericht in Streitfällen anzurufen ist und welches Recht dabei zur Anwendung kommt?	☐	☐	
Ist die Örtlichkeit der Datenhaltung beim Auftragsverarbeiter eindeutig bestimmt und schriftlich festgehalten?	☐	☐	
Ist die Zugangskontrolle am Ort der Auftragsverarbeitung gewährleistet (z. B. durch Einsatz von Schließkontaktsystemen, Einbruchmeldeanlagen, revisionsfähige Schlüsselvergabe, Zutrittsregelungen)?	☐	☐	
Ist die Zugriffsrechtevergabe auf eventuell ausgelagerte Datenbestände revisionsfähig geregelt und dokumentiert?	☐	☐	

Checkliste Auftragsverarbeitung

Frage	Ja	Nein	Anmerkungen
Existieren Vorgaben bezüglich der Benutzereinrichtung, der Änderung von Benutzerberechtigungen und der Vorgehensweise bei einem Ausscheiden von Benutzern?	☐	☐	
Wurden und werden geeignete Maßnahmen zur Gewährleistung der Zugangs- und Zugriffskontrolle ergriffen (z. B. Anmeldung mittels eindeutiger Benutzer-Identifikation, Authentisierung eines Benutzers mittels Passwort und/oder Chipkarte, revisionsfähige Anmelde- und Zugriffsaufzeichnungen)?	☐	☐	
Ist gewährleistet, dass jeder Beschäftigte des Auftragsverarbeiters nur auf die Daten des Verantwortlichen zugreifen darf, die er zur Erfüllung seiner Aufgaben benötigt?	☐	☐	
Sind besonders schützenswerte Daten durch organisatorische und technische Maßnahmen (z. B. verschlüsselte Datenspeicherung) vor einer Einsichtnahme durch das Personal des Auftragsverarbeiters geschützt?	☐	☐	
Wurden bzw. werden Maßnahmen zur Notfallvorsorge festgelegt und ergriffen?	☐	☐	
Liegt ein detailliertes Notfallkonzept vor?	☐	☐	
Wird dieses Notfallkonzept regelmäßig auf Aktualität und Angemessenheit überprüft und getestet?	☐	☐	
Ist die Aufbewahrungsdauer von Daten und Datenträgern beim Auftragsverarbeiter geregelt?	☐	☐	
Wurden dabei die gesetzlichen Anforderungen berücksichtigt?	☐	☐	
Sind die Rückgabe der Daten(träger) und Unterlagen vertraglich geregelt?	☐	☐	
Wurden und werden die betroffenen Personen bezüglich der Auslagerung ihrer Daten bzw. der Datenverarbeitung informiert?	☐	☐	
Sind die Rechte der betroffenen Personen v. a. bezüglich Auskunft, Berichtigung und Löschung im Rahmen der Auftragsverarbeitung gewährleistet?	☐	☐	
Erfolgt eine regelmäßige Kontrolle der Auftragsverarbeitung durch den Verantwortlichen?	☐	☐	
Werden die Ergebnisse der Auftragsverarbeitung zumindest stichprobenartig auf Richtigkeit überprüft?	☐	☐	
Ist der Auftragsverarbeiter dazu verpflichtet, den Verantwortlichen schriftlich über Verfahrensveränderungen und Probleme (z. B. bezüglich der Datensicherheit) im Rahmen der Auftragsverarbeitung zu informieren?	☐	☐	
Informiert der Verantwortliche den Auftragsverarbeiter über Veränderungen von vertragsrelevanten Vorhaben und Daten, zum Beispiel bei Veränderungen gesetzlicher Grundlagen?	☐	☐	