Der Bayerische Landesbeauftragte
für den Datenschutz

Leitfaden zum Outsourcing kommunaler IT

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. Claus Peter Haag | Elfriede Fograscher
Angelika Müller | Corina Scheiter

Version 1.0 | Stand: 1. März 2021

Dieses Arbeitspapier wird ausschließlich in elektronischer Form bereitgestellt. Es 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.

Inhaltsverzeichnis

1 Vorbemerkung

Dieser auf meine und auf Anregung des Bayerischen Kommunalen Prüfungsverbands in einer Arbeitsgruppe unter Mitwirkung des Bayerischen Staatsministeriums des Innern, für Sport und Integration, von Vertretern der kommunalen Spitzenverbände, des Bayerischen Kommunalen Prüfungsverbands, des Landesamts für Sicherheit in der Informationstechnik und mir erarbeitete Leitfaden soll die Kommunen bei der Auslagerung der kommunalen Informationstechnologie unterstützen. Der Leitfaden richtet sich an Kommunen, die eine solche Auslagerung in Betracht ziehen. Nicht Gegenstand ist der (mittelbare oder unmittelbare, vollständige oder partielle) Anschluss an das Bayerische Behördennetz sowie Zusammenschlüsse in kommunalen Behördennetzen. Der Kriterienkatalog erfasst also insbesondere nicht den Fall, das Landratsämter „ihren" Kommunen Hilfestellungen im Hinblick auf deren IT geben.

2 Kriterienkatalog

Nachfolgend werden die Kriterien, nach denen eine Auslagerung zu prüfen ist, in verschiedene Bereiche aufgeteilt. In der Praxis sind diese Bereiche nicht strikt voneinander zu trennen, sondern gehen vielmehr ineinander über. Insbesondere formulieren sowohl das Datenschutzrecht (Datenschutz-Grundverordnung – DSGVO) als auch das Haushaltsrecht (Kommunalhaushaltsverordnung-Kameralistik – KommHV-Kameralistik und Kommunalhaushaltsverordnung-Doppik – KommHV-Doppik) zu beachtende technisch-organisatorische Maßnahmen, die hier unter „Technisch-Organisatorische Kriterien" zusammengefasst werden.

2.1 Kriterien aus spezialgesetzlichen Regelungen

2.1.1 Meldedaten

Im Hinblick auf das Führen des Melderegisters ergeben sich die Grenzen des IT-Outsourcings aus den melderechtlichen Vorgaben. Nach § 2 Abs. 2 Bundesmeldegesetz (BMG), Art. 1 Abs. 1 Satz 1 Bayerisches Gesetz zur Ausführung des Bundesmeldegesetzes (BayAGBMG) führen die Gemeinden als Meldebehörden zur Erfüllung ihrer Aufgaben das Melderegister. Das „Führen" setzt dabei vom Ausgangspunkt voraus, dass diese Aufgabe in der durch nichts eingeschränkten rechtlichen und faktischen Herrschaft der Meldebehörde erfüllt wird oder aber eine gemäß Art. 3 Abs. 1 BayAGBMG zulässige Übertragung von Aufgaben, die **über eine Auftragsverarbeitung hinausgeht**, vorliegt. Unterhalb der Schwelle der Aufgabenübertragung gemäß Art. 3 BayAGBMG besteht die Möglichkeit der **Auftragsverarbeitung gemäß Art. 2 Abs. 1 BayAGBMG**. Art. 2 Abs. 2 BayAGBMG lässt darauf schließen, dass auch für Meldedaten eine Auftragsverarbeitung die Speicherung von Daten der Einwohner umfassen kann. Insoweit legt auch Nr. 2.2.1 Allgemeine Verwaltungsvorschrift zur Durchführung des Bundesmeldegesetzes (BMGVwV) fest: Zum Melderegister gehören auch Einwohnerdatenbestände, die die Meldebehörden bei anderen Stellen **im Rahmen der Auftragsdatenverarbeitung** führen lassen.

Da es sich hierbei aber um sensible Basisdaten zur Identität und zu den Wohnungen von Einwohnern handelt, hat die für die Datenverarbeitung verantwortliche Gemeinde im Falle einer Auslagerung des kompletten Datenbestandes diesem Umstand bei der Festlegung angemessener Sicherheitserfordernisse im Sinne der Art. 24, 25, 32 DSGVO sowie Art. 28 DSGVO Rechnung zu tragen. Sofern die Daten daher nicht in den Räumen der zuständigen Gemeinde verarbeitet und keine eigenen Speicherressourcen eingesetzt werden, ist besonderes Augenmerk auf die Datensicherheit zu legen, was in diesem Anforderungskatalog im Einzelnen erläutert wird.

2.1.2 Steuerdaten

Bei der Verwaltung von Realsteuern (nach § 3 Abs. 2 Abgabenordnung – AO – Grundsteuer und Gewerbesteuer), kommunalen Steuern und Fremdenverkehrsbeiträgen gilt das steuerliche Offenbarungsverbot gemäß § 30 AO. Dies ergibt sich aus § 1 Abs. 2 Nr. 1 AO und Art. 13 Abs. 1 Satz 1 Buchst. c Kommunalabgabengesetz (KAG). Nach § 30 Abs. 9 AO dürfen die Finanzbehörden sich bei der Verarbeitung geschützter Daten nur dann eines Auftragsverarbeiters bedienen, wenn diese Daten ausschließlich durch Personen verarbeitet werden, die zur Wahrung des Steuergeheimnisses verpflichtet sind. Soweit diese Personen nicht bereits als Amtsträger (vgl. §§ 7, 30 Abs. 1 AO) oder Gleichgestellte (vgl. § 30 Abs. 3 AO) zur Wahrung des Steuergeheimnisses verpflichtet sind, sind Auftragsverarbeiter bzw. Beschäftigte des Auftragsverarbeiters nach dem Verpflichtungsgesetz zu verpflichten. Im **Vertrag** über die Auftragsverarbeitung muss zudem festgelegt werden, dass **ausschließlich** diese besonders **verpflichteten Personen** tätig werden und der Einsatz von nicht verpflichtetem Personal auch bei Beteiligung von weiteren Auftragsverarbeitern ausgeschlossen ist.

2.1.3 Sozialdaten

Im Hinblick auf die Verarbeitung von Sozialdaten im Auftrag ist § 80 Zehntes Buch Sozialgesetzbuch – Sozialverwaltungsverfahren und Sozialdatenschutz – (SGB X) zu beachten. Nach § 80 Abs. 1 Satz 1 SGB X ist **vor Erteilung eines Auftrags** dieser **rechtzeitig** gegenüber der Rechts- oder Fachaufsichtsbehörde **anzuzeigen**. Die Anzeigepflicht gilt nach § 80 Abs. 1 Satz 2 SGB X auch für öffentliche Stellen, welche Auftragnehmer werden. In einem solchen Fall gleichsam doppelter Anzeigepflichten sollte auf eine enge inhaltliche Abstimmung der beiden erforderlichen Anzeigen geachtet werden. Wer insoweit Verantwortlicher im Rahmen des § 80 SGB X ist, wird durch § 35 Abs. 1 Erstes Buch Sozialgesetzbuch – Allgemeiner Teil – (SGB I) vorgegeben. Der Verantwortliche hat umfassend die Pflicht, dass alle Vorgaben des speziellen Sozialdatenschutzes nach § 35 SGB I in Verbindung mit §§ 67 ff. SGB X unter Beachtung der allgemeingültigen Regelungen des Art. 28 DSGVO eingehalten werden. Hierbei ist insbesondere § 67 Abs. 4 SGB X zu beachten (Verantwortlichkeit der Leistungsträger im Sinne von § 12 SGB I). Im Falle von § 67 Abs. 4 Satz 2 SGB X (Leistungsträger ist eine Gebietskörperschaft, z. B. Land, Kreis, Bezirk oder Stadt) hat dies zur Folge, dass die jeweilige Organisationseinheit verantwortlich ist, die eine Aufgabe funktional durchführt (z. B. Wohnungs-, Jugend- oder Sozialamt). Jede dieser Organisationseinheiten der Gebietskörperschaft kann damit eine andere (eigene) verantwortliche Stelle sein. Diese Stelle ist dann auch dafür verantwortlich, die Anforderungen zur Verarbeitung von Sozialdaten im Auftrag zu erfüllen, insbesondere eine eigene Vereinbarung im Sinne von Art. 28 Abs. 3 DSGVO zu schließen.

Des Weiteren ist zu beachten, dass ein Auftrag gemäß § 80 Abs. 2 SGB X nur dann erteilt werden darf, wenn die Verarbeitung im Inland, in einem anderen Mitgliedstaat der Europäischen Union, in einem diesem nach § 35 Abs. 7 SGB I gleichgestellten Staat oder, sofern ein Angemessenheitsbeschluss gemäß Art. 45 DSVGO vorliegt, in einem Drittstaat oder in einer internationalen Organisation erfolgt. Dadurch soll **ausgeschlossen** werden, dass Sozialdaten in **unsichere Drittstaaten** übermittelt werden.

Darüber hinaus verlangt § 80 Abs. 3 SGB X eine gesonderte Prüfung der Zulässigkeit der Auftragsverarbeitung im Falle der Verarbeitung von Sozialdaten durch **nichtöffentliche Stellen** (Ausnahme: siehe § 80 Abs. 5 SGB X). Danach ist eine Auftragserteilung **nur zulässig**, wenn beim Verantwortlichen sonst **Störungen im Betriebsablauf** auftreten können oder die übertragenen Arbeiten beim Auftragsverarbeiter **erheblich kostengünstiger** besorgt werden können. Unter Störungen im Betriebsablauf versteht der Gesetzgeber abstrakt Ereignisse, die die Abwicklung der Leistungen zu Lasten des Leistungsempfängers verzögern.[1] Eine entsprechende Störung kann wohl auch bei einem besonders großen Arbeitsanfall, z. B. wegen umzusetzender Gesetzesänderungen vorliegen. Um eine Kostenersparnis im Sinne von § 80 Abs. 3 Satz 1 Nr. 2 SGB X bejahen zu können, bedarf es bezüglich der Datenverarbeitung einer Vergleichsberechnung hinsichtlich der zu erwartenden Kosten beim Verantwortlichen einerseits und dem Auftragsverarbeiter andererseits. Dabei sind sämtliche zu erwartenden Kosten einzubeziehen (z. B. Hard- und Softwarekosten, Personal- und Gebäudekosten). Entscheidend ist am Ende, dass die Auftragsverarbeitung erheblich kostengünstiger ist als die eigene Datenverarbeitung des Verantwortlichen. Was unter dem Begriff „erheblich" zu verstehen ist, ist gesetzlich nicht näher definiert und muss im jeweils konkreten Einzelfall geprüft werden. Unter Berücksichtigung des Gesetzeszwecks (weitgehende Begrenzung der Datenverarbeitung durch nichtöffentliche Stellen) sowie des Sozialdatenschutzes muss sich aber grundsätzlich eine Ersparnis ergeben, die bei objektiver Betrachtung die eigene Datenverarbeitung des Verantwortlichen unwirtschaftlich erscheinen lassen würde.

Das Ergebnis dieser Prüfung ist in nachprüfbarer Form zu dokumentieren. Zudem ist der Rechtsgedanke des § 78 SGB X zu beachten, wonach das hohe Schutzniveau für Sozialdaten auch dann gilt, wenn diese den Schutz- und Verantwortungsbereich des Sozialleistungsträgers verlassen.

2.1.4 Personalaktendaten

Sofern Personalaktendaten durch den Auftragsverarbeiter verarbeitet werden sollen, sind § 50 Beamtenstatusgesetz und Art. 103 ff. Bayerisches Beamtengesetz (BayBG) zu beachten. Diese beamtenrechtlichen Regelungen gelten nach Art. 145 Abs. 2 BayBG im Wesentlichen entsprechend für vertraglich beschäftigte Personen im Dienst einer der in Art. 1 Abs. 1 BayBG genannten juristischen Person des öffentlichen Rechts (Staat, Gemeinden, Gemeindeverbände, sonstige unter der Aufsicht des Staates stehende Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts). Art. 108 Abs. 3 Satz 1 BayBG regelt die Voraussetzungen, unter denen sich eine personalverwaltende Stelle eines Auftragsverarbeiters im Sinne des Art. 4 Nr. 8 DSGVO bedienen darf. Nach Art. 108 Abs. 3 Satz 1 BayBG ist eine Auftragsverarbeitung in Bezug auf Personalaktendaten nur zulässig, **soweit** sie als **unterstützende Dienstleistung** im Rahmen der überwiegend automatisierten Erledigung von Aufgaben der Behörde zur **Vermeidung von Störungen** im Geschäftsablauf des Dienstherrn oder zur Realisierung **erheblich wirtschaftlicherer Arbeitsabläufe erforderlich** ist. Die Prüfung dieser Voraussetzung ist in nachprüfbarer Form zu dokumentieren. Die Vorgaben für die konkrete Ausgestaltung der Auftragsverarbeitung ergeben sich unmittelbar aus Art. 28 und 29 DSGVO.

[1] Vgl. BT-Drs. 14/4329, S. 52.

Art. 108 Abs. 3 Satz 2 BayBG bestimmt zusätzlich für die Fälle, in denen nicht öffentliche Stellen als Auftragsverarbeiter beauftragt werden, dass die mit der Verarbeitung von Personalaktendaten befassten Beschäftigten nach dem Verpflichtungsgesetz zur Wahrung der Daten verpflichtet werden. Die personalverwaltende Behörde bleibt auch bei Einschaltung eines Auftragsverarbeiters stets „Verantwortlicher" für die Datenverarbeitung im Sinne von Art. 4 Nr. 7 DSGVO.

2.1.5 Ordnungswidrigkeiten

Eine Auftragsverarbeitung im Rahmen der Ordnungswidrigkeitenverfolgung und -ahndung erfolgt nicht im Anwendungsbereich der Datenschutz-Grundverordnung, sondern im Anwendungsbereich der **Datenschutz-Richtlinie für Polizei und Strafjustiz** (RLDSJ).[2] Diese Richtlinie wurde sowohl auf Landes- als auch auf Bundesebene in den jeweiligen Fachgesetzen umgesetzt. Sofern also Kommunen Ordnungswidrigkeiten verfolgen und ahnden gelten für die hiermit verbundenen Datenumgänge das Ordnungswidrigkeitengesetz (OWiG) sowie über Verweisungen – in der Regel § 46 Abs. 1 OWiG – auch die Strafprozessordnung (StPO), vgl. Art. 1 Abs. 5 Bayerisches Datenschutzgesetz (BayDSG) und die Subsidiaritätsklausel in Art. 28 Abs. 1 Satz 1 BayDSG („soweit nichts anderes bestimmt ist").

Mit Umsetzung der Datenschutz-Richtlinie für Polizei und Strafjustiz in das Bundesrecht im November 2019 wurde unter anderem § 500 StPO neu eingeführt. Dieser ist auch im Ordnungswidrigkeitenverfahren anwendbar (§ 46 Abs. 1 OWiG). § 500 StPO verweist seinerseits ergänzend auf das 3. Kapitel des Bundesdatenschutzgesetzes (BDSG). Damit sind im Ordnungswidrigkeitenverfahren auch die §§ 45 ff. BDSG zu berücksichtigen, soweit das Ordnungswidrigkeitengesetz und die Strafprozessordnung keine spezielleren Regelungen treffen. **Für den Bereich der Auftragsverarbeitung gilt** über die Verweisungskette des § 46 Abs. 1 OWiG, § 500 Abs. 1 StPO der **§ 62 BDSG**. § 62 BDSG regelt die Voraussetzungen einer zulässigen Auftragsverarbeitung. Die **Anforderungen an die Sicherheit der Datenverarbeitung** regelt im Ordnungswidrigkeitenverfahren **§ 64 BDSG** in Verbindung mit § 46 Abs. 1 OWiG, § 500 StPO. Es wird darauf hingewiesen, dass sich in der Praxis Art. 28 DSGVO und § 62 BDSG dahingehend unterscheiden, dass § 62 BDSG keinen Nachweis der einzuhaltenden Garantien durch genehmigte Verhaltensregeln oder Zertifizierungsverfahren sowie die Möglichkeit der Einführung von Standardvertragsklauseln vorsieht. **Erforderlich ist daher eine sorgfältige Auswahl und Überprüfung des Auftragsverarbeiters, insbesondere hinsichtlich der technischen und organisatorischen Maßnahmen** nach § 64 BDSG in Verbindung mit § 46 Abs. 1 OWiG, § 500 StPO.

Ergänzend zu § 62 BDSG wird die Auftragsverarbeitung im Zusammenhang mit der **dauerhaften rechtsverbindlichen Speicherung elektronischer Akten** im Ordnungswidrigkeitenverfahren durch **§ 497 Abs. 1, 2 StPO in Verbindung mit § 49d OWiG** geregelt. In den

[2] 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).

Anwendungsbereich des § 497 Abs. 1, 2 StPO fällt eine dauerhafte, rechtsverbindliche Speicherung elektronischer Akten im Sinne des § 110a OWiG durch nichtöffentliche Stellen als Auftragsverarbeiter. Diese erfolgt regelmäßig in zentralen Rechenzentren.[3]

Bloße nicht rechtsverbindliche elektronische Aktenkopien, die neben der lückenlosen Papierakte bestehen, werden dagegen nicht erfasst. Eine dauerhafte rechtsverbindliche Speicherung elektronischer Akten im Ordnungswidrigkeitenverfahren im Sinne des § 110a OWiG ist nur dann zulässig, wenn die öffentliche Stelle den **Zutritt und den Zugang zu den Datenverarbeitungsanlagen**, in denen die elektronischen Akten rechtsverbindlich gespeichert werden, **tatsächlich und ausschließlich kontrolliert (§ 497 Abs. 1 StPO)**. Ist dies nicht der Fall, ist ein Outsourcing an andere als öffentliche Stellen nicht möglich.

2.1.6 Prüfungsrechte

Das Ermitteln von Ansprüchen und Zahlungsverpflichtungen, das Vorbereiten der entsprechenden Kassenanordnungen, die Abwicklung der Kassengeschäfte und des Rechnungswesens sowie die Aufbewahrung von elektronischen Belegen sind heutzutage ohne den Einsatz von Informationstechnik kaum noch denkbar. Wenn die Kommune die hierzu erforderlichen technischen Hilfstätigkeiten (z. B. Hosting des zentralen Finanzwesens oder anderer finanzwirksamer Verfahren im Sinne von § 37 Abs. 1 KommHV-Kameralistik/§ 33 Abs. 1 KommHV-Doppik, elektronisch geführte Bücher, Vorbücher oder weitere Bücher im Sinne der §§ 65, 67 und 69 KommHV-Kameralistik/§§ 61, 63 und 65 KommHV-Doppik oder elektronisch aufbewahrte Belege im Sinne von § 71 Abs. 1 KommHV-Kameralistik/§ 67 KommHV-Doppik) teilweise oder vollständig auf Dritte verlagert, sind von der beauftragenden Kommune **Art. 101 GO** oder die vergleichbaren Bestimmungen in anderen Kommunalgesetzen (vgl. **Art. 87 LKrO, Art. 83 BezO**) zu beachten.

Danach muss auch bei einem Outsourcing finanzwirksamer automatisierter Verfahren, elektronischer Bücher und Belege sichergestellt sein, dass eine **ordnungsmäßige und sichere Erledigung und die Prüfung nach den für die Kommune geltenden Vorschriften** gewährleistet sind. Insbesondere wäre von der Kommune darauf zu achten, dass vom Auftragsverarbeiter die in § 37 Abs. 1 Nr. 3 bis 9, § 43 Abs. 1 Nr. 3, § 62 Abs. 1 Satz 3, § 71 Abs. 2 Satz 1, Abs. 4 und § 82 Abs. 4 KommHV-Kameralistik/§ 33 Abs. 1 Nr. 3 bis 9, § 39 Abs. 1 Nr. 3, § 58 Abs. 1 Satz 3, § 67 Abs. 2 Satz 1, Abs. 4 und § 69 Abs. 4 KommHV-Doppik genannten haushaltsrechtlichen Verpflichtungen durch geeignete technische und organisatorische Maßnahmen eingehalten werden.

Ebenso müssen sich nach den oben genannten Bestimmungen die für die örtliche Prüfung im Sinne des Art. 103 GO und die überörtliche Prüfung im Sinne des Art. 105 GO zuständigen Prüfungsorgane von der ordnungsmäßigen Erledigung der übertragenen Geschäfte insbesondere nach Maßgabe von Art. 106 sowie Art. 120 Abs. 1 GO in Verbindung mit der Kommunalwirtschaftliche Prüfungsverordnung (KommPrV) vergewissern können. Dies wäre

[3] BT-Drs. 18/9416, S. 68.

über eine entsprechende vertragliche Vereinbarung mit dem Auftragsverarbeiter sicherzustellen. Auf § 6 KommPrV sowie die dazu ergangenen Verwaltungsvorschriften[4] wird hingewiesen.

2.2 Allgemeine Kriterien aus dem Datenschutzrecht

Aus datenschutzrechtlicher Sicht ergeben sich die allgemeinen Kriterien für eine Auslagerung der IT insbesondere aus Art. 28 DSGVO, der die Auftragsverarbeitung regelt. Faktisch wird ein IT-Outsourcing regelmäßig nur unter Gebrauchmachen von diesem in der Datenschutz-Grundverordnung enthaltenen Modell möglich sein, da die Verarbeitung personenbezogener Daten durch den IT-Dienstleister nicht ausgeschlossen werden kann und es regelmäßig auch nicht soll (zu Ausnahmen siehe unter Nr. 2.4.4.2 A.6). Auftragsverarbeitung liegt vor, wenn eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet (siehe Definition Auftragsverarbeiter in Art. 4 Nr. 8 DSGVO). Ein Auftragsverarbeitungsvertrag zum Outsourcing kommunaler IT muss daher zunächst einmal alle Voraussetzungen erfüllen, die allgemein an Auftragsverarbeitungsverhältnisse gestellt werden, insbesondere müssen die in Art. 28 Abs. 3 DSGVO genannten Mindestinhalte eines Auftragsverarbeitervertrages beachtet werden.[5] Insbesondere ist zu beachten:

2.2.1 Sorgfältige Auswahl des Auftragsverarbeiters

Die Kommunen müssen auf eine sorgfältige Auswahl der Dienstleister achten. Nach Art. 28 Abs. 1 DSGVO darf nur ein Auftragsverarbeiter ausgewählt werden, der hinreichende Garantien für eine datenschutzkonforme Verarbeitung bietet. Insbesondere sind hierbei folgende Punkte zu beachten:

- Eine insbesondere Aspekte der IT-Sicherheit umfassende Zertifizierung des Auftragnehmers ist regelmäßig erforderlich (hierzu konkreter unter Nr. 2.4.4.4 A.12). Ausnahmen sind aber möglich, da zuzugeben ist, dass es derzeit keine Zertifizierung gibt, die alle Voraussetzungen der Datenschutz-Grundverordnung umfasst. Sollte in einem Ausnahmefall ein Auftragsverarbeiter ohne Zertifizierung beauftragt werden, muss der Anforderungskatalog vollständig überprüft und bejaht werden, ohne dass einzelne Punkte unter Berufung auf eine vorhandene Zertifizierung als erfüllt gelten können.
- Der IT-Dienstleister muss (z. B. durch ausreichende personelle Ausstattung auch nachts, an Feiertagen und Wochenenden) gewährleisten, dass im Bedarfsfall ein ununterbrochener, zuverlässiger 7/24-Betrieb der IT möglich ist.

[4] Bekanntmachung des Bayerischen Staatsministeriums des Innern über die Verwaltungsvorschriften zur Kommunalwirtschaftlichen Prüfungsverordnung vom 26. November 1981 (MABl. S. 740), die zuletzt durch Bekanntmachung vom 27. Dezember 2018 (BayMBl. 2019 Nr. 4) geändert worden ist.

[5] Siehe hierzu Bayerischer Landesbeauftragter für den Datenschutz, Auftragsverarbeitung, Orientierungshilfe, Stand 4/2019, Internet: https://www.datenschutz-bayern.de, Rubrik „Datenschutzreform 2018 – Orientierungs- und Praxishilfen – Auftragsverarbeitung".

- Der IT-Dienstleister darf nur qualifiziertes und zuverlässiges Personal einsetzen und muss seine Beschäftigten nachweislich weiterbilden.
- Der IT-Dienstleister muss kompetente Ansprechpartner für Datenschutz und IT-Sicherheit vorweisen; idealerweise hat er einen Datenschutzbeauftragten benannt und einen IT-Sicherheitsbeauftragten bestellt.
- Der Dienstleister sollte nachweisen, dass er von einem Warn- und Informationsdienst Informationen zu Schwachstellen in Hard- und Software erhält. Dies kann z. B. durch Weiterleitung der LSI-Warnmeldungen von der Kommune an den Dienstleister erfolgen.

Sofern vertraglich weitere Auftragsverarbeiter zugelassen werden, müssen in diesem Unterauftragsverhältnis die gleichen hohen Anforderungen sichergestellt werden.

2.2.2 Wahrung des Datengeheimnisses

Nach Art. 28 Abs. 3 S. 2 Buchst. b DSGVO bzw. § 62 Abs. 5 Satz 2 Nr. 2 BDSG muss der Auftragsverarbeiter gewährleisten, dass sich seine Beschäftigten zur Vertraulichkeit verpflichten oder einer angemessenen gesetzlichen Verschwiegenheitsverpflichtung unterliegen. Weitergehende Verschwiegenheitsverpflichtungen ergeben sich aus den bereichsspezifische Anforderungen, etwa § 7 Abs. 2 BMG, § 30 Abs. 9 AO, § 35 SGB I, Art. 108 Abs. 3 Satz 2 BayBG (vgl. dazu oben unter Nr. 2.1).

2.2.3 Sicherstellung des Zugriffs auf die Daten

Die auslagernde Kommune muss die Auslagerung so gestalten, dass sie jederzeit Zugriff auf ihre Daten hat. Der Verantwortliche ist im Verhältnis zum Auftragsverarbeiter „Herr“ über die Daten; dies muss sich auch in der praktischen Ausführung des Auftragsverarbeitungsverhältnisses widerspiegeln. Es ist daher grundsätzlich erforderlich, Klauseln in den Vertrag aufzunehmen, die den Schutz der im Auftrag des Verantwortlichen verarbeiteten personenbezogenen Daten vor Zugriffen Dritter (z. B. mittels Pfändung, Beschlagnahme, Zwangsvollstreckung oder gegebenenfalls bei Insolvenz des Auftragsverarbeiters) sicherstellen. Insbesondere hat die Kommune dafür Sorge zu tragen, dass sie nicht durch eine Insolvenz des Dienstleisters den Zugriff auf ihre Daten verliert. Sie sollte daher bei steigendem Ausmaß des Outsourcings oder hoher Sensibilität der Daten nicht nur einen jederzeitigen Herausgabeanspruch vereinbaren, sondern entweder einen Dienstleister auswählen, der nicht insolvenzfähig ist, oder durch spezielle Regelungen im Auftragsverarbeitungsvertrag Vorkehrungen treffen, die auch bei Eintreten einer Insolvenz eine schnelle Handlungsmöglichkeit sicherstellen. Das im konkreten Einzelfall erforderliche Ausmaß an Vorkehrungen hängt von der Sensibilität der Daten sowie dem Ausmaß des Outsourcings ab. Damit Auftragsverarbeitungsverhältnisse diesen erhöhten Sensibilitätserfordernissen genügen, sind verschiedene Konstellationen denkbar, etwa:

- Zusammenschluss mehrerer Kommunen und Gründung eines eigenen IT-Dienstleisters (als Körperschaft des öffentlichen Rechts);
- Nutzung eines bereits bestehenden Rechenzentrums bzw. von IT-Diensten einer anderen Kommune;

- sonstige Formen kommunaler Zusammenarbeit im Rahmen des hierfür zur Verfügung stehenden Rechtsrahmens;
- Verarbeitung und Speicherung durch einen nicht insolvenzfähigen Anbieter;
- Bei Datenverarbeitung durch einen privatwirtschaftlich organisierten Auftragsverarbeiter ist durch die Vertragsgestaltung dafür zu sorgen, dass eine Aussonderung des Datenbestandes auch im Falle der Insolvenz tatsächlich möglich ist. Dies kann bei hoher Sensibilität der betroffenen Daten bzw. einem hohen Umfang des Outsourcings z. B. den Erwerb eines eigenen NAS-Servers erfordern, der in den Räumen des Dienstleisters steht und deutlich als Eigentum der Gemeinde gekennzeichnet ist. Die Gemeinde bleibt Eigentümerin des NAS-Servers und es werden ausschließlich Daten der jeweiligen Gemeinde dort vorgehalten (sogenanntes Housing). Alternativ kann auch ein entsprechender Backupserver oder andere Backupmedien verwendet werden, die bei der Kommune verbleiben und auf der regelmäßig eine Kopie der Daten abgelegt werden. Für dieses Backup müssen allerdings analoge Schutzmaßnahmen angewendet werden wie für die Original-Server.

Dem Auftragsverarbeiter ist darüber hinaus die Pflicht aufzuerlegen, in einem absehbaren Fall von Zugriffen Dritter den Verantwortlichen unverzüglich in Kenntnis zu setzen.

2.2.4 Tatsächliche Überprüfungen

Die Kommune sollte, soweit sie keinen nach ISO 27001 (vorzugswürdig in der Ausprägung des BSI IT-Grundschutz) zertifizierten Dienstleister nutzt, sicherstellen, dass sie den Auftragsverarbeiter überprüfen und diese Überprüfungen auch tatsächlich (durch spezialisierte Mitarbeiter oder Einschaltung von unabhängigen externen Sachverständigen) durchführen kann. Genaueres siehe Nr. 2.4.4.4 A.12.

2.2.5 Erteilung fachkundiger Weisungen

Fachkundige Weisungen an den Dienstleister erstrecken sich sowohl auf Weisungen hinsichtlich der Mittel der Verarbeitung wie auch auf Definition, Beauftragen und Testen von Anforderungen als Schnittstelle zwischen Fachanwendung und IT, um die IT-gestützten Prozesse in der Kommune in der Rolle als Verantwortlicher zu gestalten. Die Kommune muss sicherstellen, dass das Weisungsrecht fachkundig ausgeübt werden kann. Als Arbeitserleichterung für die Kommune kann im Falle eines nach ISO 27001 (vorzugswürdig in der Ausprägung des BSI IT-Grundschutz) zertifizierten Dienstleisters in der Regel auf Weisungen hinsichtlich der Mittel der Verarbeitung verzichtet werden, da mit dem Zertifikat nachgewiesen wurde, das ausreichend Fachkunde auf Seiten des Dienstleisters zur sicheren Bereitstellung der Dienste vorhanden ist. Zur Erteilung fachkundiger Weisungen ist notwendig, dass der Verantwortliche ein gewisses Maß an Kenntnissen über die beauftragte Tätigkeit hat. Für diese Tätigkeit sollte der Verantwortliche einen festangestellten, in gewissem Maße technisch versierten Beschäftigten (nachweisbar durch Ausbildungen oder Berufserfahrung) benennen, der auf Augenhöhe mit dem Auftragsverarbeiter kommunizieren kann. Dazu ist es erforderlich, dass er die Fachanwendungen verstehen und gut bedienen kann, Betriebsabläufe gege-

benenfalls überwachen kann und weiß, wo und wie in Notsituationen Unterstützung angefordert wird. Konkrete Kenntnis über die Abläufe im Rechenzentrum sind dabei zwar nicht erforderlich; jedoch sollten fundierte Kenntnisse über die genutzten Fachverfahren vorhanden sein, einschließlich des Wissens, welche Verfahren betrieben werden, welche Auftragsverarbeitungsverhältnisse und welche Schnittstellen zwischen den Verfahren bestehen. Es ist also auch bei Auslagerung der kommunalen IT notwendig, dass die Kommune **Personal vorhält, das dieses technisch-organisatorische Basisfachwissen hat.** Erforderlichenfalls sind die Möglichkeiten kommunaler Zusammenarbeit im Rahmen des hierfür zur Verfügung stehenden Rechtsrahmens zu nutzen.

2.2.6 Sicherstellung von Prüfungsrechten

Darüber hinaus muss auch sichergestellt werden, dass Prüfungen (z. B. durch den Bayerischen Kommunalen Prüfungsverband oder den Bayerischen Landesbeauftragten für den Datenschutz), denen die Kommunen unterworfen sind, ohne Einschränkung wahrgenommen werden können.

2.2.7 Regelung einer Rückgabe der Daten

Es muss explizit geregelt werden, was mit den Daten nach Beendigung des Vertrages passiert. Art. 28 Abs. 3 S. 2 Buchst. g DSGVO fordert, dass nach Beendigung die Daten nach Wahl des Verantwortlichen zurückgegeben oder gelöscht werden müssen, sofern nicht eine gesetzliche Pflicht zur Speicherung besteht. Wenn es sich nicht lediglich um ein nicht mehr erforderliches Backup des Datenbestandes beim Dienstleister handelt, ist jedenfalls eine ohne vorherige Anweisung der Kommune erfolgende Datenlöschung auszuschließen. Die Bedeutung der Daten erfordert hier eine konkrete Regelung. Voraussichtlich wird in diesen Fällen regelmäßig eine Rückgabe erforderlich sein. Darüber hinaus ist – beispielsweise durch Bezugnahme auf das IT-Sicherheitskonzept des Dienstleisters – zu regeln, wie einem dauerhaften Verlust der Daten wirksam vorgebeugt wird und was bei einem Datenverlust (beispielsweise einem Ransomware-Angriff) geschieht.

2.2.8 Technisch-Organisatorische Aspekte

Die Regelungen der Art. 24, 25 und 32 DSGVO zu Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen und zur Sicherheit der Verarbeitung müssen eingehalten werden. Zudem ist durch eine entsprechende systematische, risikobasierte Erforderlichkeitsprüfung zu klären, ob eine Datenschutz-Folgenabschätzung nach Art. 35 DSGVO erforderlich ist. Diese ist im Bedarfsfall vorab durchzuführen. Konkretisierungen hierzu finden sich unter Nr. 2.4.1.

2.3 Allgemeine Kriterien aus dem Haushalts- und Steuerrecht

Auch wenn Tätigkeiten aus dem Bereich der kommunalen Verwaltung durch einen Auftragsverarbeiter durchgeführt werden, sind weiterhin die sich aus dem Haushaltsrecht ergebenden Verpflichtungen einzuhalten. Diese Verpflichtungen obliegen der Kommune selbst. Um sie einzuhalten, muss die Kommune ggf. auch den Auftragsverarbeiter vertraglich zur Mitwirkung verpflichten. Insbesondere muss die Gemeinde darauf achten, folgende Verpflichtungen erfüllen zu können:

2.3.1 Haushaltsrechtliche Grundsätze

Die Einhaltung allgemeiner haushaltsrechtlicher Grundsätze ist auch bei Auftragsverarbeitung sicherzustellen. Dabei ist auf Folgendes zu achten:

- die Sicherheit, Verfügbarkeit, Vertraulichkeit und Integrität der finanzwirksamen Verfahren sowie der eingesetzten Zahlungs- und Kassensysteme;
- die Sicherung und Wiederherstellbarkeit der automatisierten Verfahren und deren Datenbanken;
- den ordnungsgemäßen Einsatz der finanzwirksamen Verfahren, Zahlungs- und Kassensysteme entsprechend den haushaltsrechtlichen oder bereichsspezifischen Bestimmungen;
- die Klarheit, Wahrheit, Sicherheit und Nachvollziehbarkeit der elektronischen Buchführung;
- die technischen und organisatorischen Maßnahmen, die der inneren Kassensicherheit dienen (siehe hierzu auch Nr. 2.4);
- die Revisionsfähigkeit der finanzwirksamen Geschäftsprozesse, automatisierten Verfahren sowie der elektronischen Akten- und Belegführung.

Im Hinblick auf automatisierte Verfahren sind für die Kommunen § 33 KommHV-Doppik und § 37 KommHV-Kameralistik zu beachten.

2.3.2 Kommunale Buchführung

Die sich aus den haushaltsrechtlichen Grundsätzen ordnungsmäßiger kommunaler Buchführung und den Bestimmungen zur Sicherung der Bücher ergebenden Anforderungen sind einzuhalten (vgl. §§ 61, 62 Abs. 1 Satz 3 KommHV-Kameralistik, §§ 57, 58 Abs. 1 Satz 3 KommHV-Doppik).

2.3.3 Steuerliche Buchführungspflichten

Bestehen für die Kommune steuerliche Buchführungs- und Aufzeichnungspflichten aus der Abgabenordnung oder aus Einzelsteuergesetzen, sind auch die in den Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen

in elektronischer Form sowie zum Datenzugriff festgelegten Anforderungen zu berücksichtigen.[6]

2.3.4 Belege

Die Anforderungen an die elektronische Aufbewahrung von Belegen sind zu beachten (vgl. § 71 Abs. 2 und 4 KommHV-Kameralistik, § 67 Abs. 2 und 4 KommHV-Doppik).

2.3.5 Wechsel zu anderen Verfahren

Bei einem Wechsel zwischen automatisierten Verfahren oder zwischen Dienstleistern sind alle Anforderungen einzuhalten, die eine maschinelle Auswertbarkeit der Bücher und Belege für die Dauer der gesetzlichen Ausbewahrungspflichten gewährleisten sollen (vgl. § 82 Abs. 4 KommHV-Kameralistik, § 69 Abs. 4 KommHV-Doppik).

2.3.6 Nachvollziehbarkeit

Da es für die Ordnungsmäßigkeit, Sicherheit, Wirtschaftlichkeit der Buchführung und deren Revisionsfähigkeit entscheidend auf die Nachvollziehbarkeit der Geschäftsvorfälle in ihrer Entstehung und Abwicklung ankommt, wird großer Wert gelegt auf eine ordnungsgemäße Aktenführung. Für die elektronische Führung von Akten, Vorgängen und Dokumenten werden die in Art. 7 Bayerisches E-Government-Gesetz (BayEGovG) genannten allgemeinen Anforderungen bzw. vorrangig etwaige bereichsspezifische Bestimmungen zugrundegelegt.

2.4 Technisch-Organisatorische Kriterien

An dieser Stelle werden technisch-organisatorische Voraussetzungen zusammengefasst, die sich aus Art. 24, 25 und 32 DSGVO, § 33 KommHV-Doppik, § 37 KommHV-Kameralistik und aus den Grundsätzen der IT-Sicherheit ergeben. Der Auftragsverarbeiter hat alle erforderlichen technischen Maßnahmen zu treffen. Dies muss von der **Kommune grundsätzlich überprüft** werden, da sie trotz Outsourcings als **Verantwortliche** die Maßnahmen nach Art. 32 DSGVO bzw. im Ordnungswidrigkeitenverfahren nach § 64 BDSG in Verbindung mit § 46 Abs.1 OWiG, § 500 StPO sowie ggf. § 497 StPO umsetzen muss.

Der Verantwortliche muss durch eine entsprechende **systematische, risikobasierte Erforderlichkeitsprüfung** klären, ob eine Datenschutz-Folgenabschätzung nach Art. 35 DSGVO bzw. im Ordnungswidrigkeitenverfahren nach § 67 BDSG in Verbindung mit § 46 Abs. 1 OWiG, § 500 StPO durchzuführen ist und diese im Bedarfsfall vorab durchführen. Der IT-Dienstleister legt zudem ein **ausführliches Sicherheitskonzept** vor, das von der Kommune genehmigt werden muss. Im Rahmen der Zertifizierung nach ISO 27001 (vorzugswürdig in der Ausprägung des BSI IT-Grundschutz) liegt ein derartiges Sicherheitskonzept in der Regel vor. Besitzt der ausgewählte Dienstleister keine entsprechende Zertifizierung, muss bezüglich der Systematik und inhaltlichen Tiefe ein äquivalentes Sicherheitskonzept erstellt werden.

[6] Vgl. Bundesministerium der Finanzen, Schreiben vom 28. November 2019, BStBl I 2019, S. 1269 ff..

Eine gegebenenfalls vorliegende **Sicherheitszertifizierung** des IT-Dienstleisters kann im Rahmen der behördlichen Risikoanalyse als Faktor **berücksichtigt werden**. Eine einheitliche Zertifizierung der Dienstleister für die unterschiedlichen Szenarien des IT-Outsourcings ist derzeit jedoch nicht möglich. Da sich die Zielrichtung der verschiedenen angebotenen Zertifizierungen unterscheiden, ist jeweils zu prüfen, ob die Zertifizierung für den Zweck geeignet ist, ob also die Zielrichtung der Zertifizierung mit dem geplanten Zweck (Scope) übereinstimmt. Zudem ist derzeit noch keine Datenschutzzertifizierung nach Art. 42 DSGVO vorhanden. Ist eine vorhandene Zertifizierung für den Zweck des Outsourcings relevant, ist in einem zweiten Schritt auch der Umfang der Zertifizierung, also die geprüften Kriterien und der Schutzbedarf der ausgelagerten Verarbeitungen, einer Prüfung zu unterziehen. Zur Erleichterung für die Praxis wird diesem Anforderungskatalog ein Anhang beigefügt, der für einige Szenarien erläutert, welche Zertifizierung von Vorteil ist und ob gegebenenfalls einige der Anforderungen mit der Zertifizierung bereits abgedeckt sind.

2.4.1 Risikoanalyse

Bei der erforderlichen **Risikoanalyse** der Kommune ist **zunächst** anhand der auszulagernden Daten zu ermittelten, welche rechtlichen Regelungen umzusetzen sind und welcher **Schutzbedarf** damit angenommen werden muss. Einen aus Datenschutzsicht hohen Schutzbedarf haben besondere Kategorien von personenbezogenen Daten nach Art. 9 Abs. 1 DSGVO (beispielsweise Gesundheitsdaten) sowie Datenkategorien mit spezialgesetzlichen Regelungen (Meldedaten, Steuerdaten, Personaldaten, Daten aus Ordnungswidrigkeitenverfahren, Sozialdaten usw.). Ein anderer – nicht datenschutzrechtlicher – Grund für die Anwendung eines hohen Schutzbedarfs kann zum Beispiel die Einstufung als kritische Infrastruktur sein. Hierbei ist das Maximalprinzip zu beachten: ist für eine Datenkategorie der Schutzbedarf als hoch ermittelt worden, so ist der Schutzbedarf für den gesamten Informationsverbund – für alle damit zusammenhängenden Daten, Verarbeitungsvorgänge und IT-Geräte – als hoch zu werten.

Unter Nr. 2.4.4 werden Anforderungen definiert, die aus den Besonderheiten mit dem teilweise hohen Schutzbedarf der einzelnen Datenkategorien z. B. aus dem Meldewesen, dem Sozial- bzw. Gesundheitsbereich oder der Ordnungswidrigkeitenverfolgung resultieren.

Die Risikoanalyse wird unter Berücksichtigung des Auslagerungsszenarios (siehe Nr. 2.4.2) fortgesetzt. Für die erforderliche Risikoanalyse wird auf die Orientierungshilfe „Datenschutz-Folgenabschätzung“ verwiesen.[7]

Ist die Risikoanalyse abgeschlossen, können die unter Nr. 2.4.4 genannten Maßnahmen als risikomindernd betrachtet werden.

2.4.2 Gängige Varianten für Outsourcing

Die zu erfüllenden Anforderungen bei der Auslagerung bestimmen sich insbesondere danach, welche Verarbeitungen die Kommune auslagern will. Da das Auslagerungsszenario ein

[7] Bayerischer Landesbeauftragter für den Datenschutz, Datenschutz-Folgenabschätzung, Orientierungshilfe, Stand 2/2021, Internet: https://www.datenschutz-bayern.de, Rubrik „DSFA“.

wichtiges Kriterium für die Bestimmung der umzusetzenden Maßnahmen darstellt, werden die unterschiedlichen Outsourcing Varianten kurz aufgeführt:

Folgende klassische Outsourcing-Varianten sind üblich:

- Webhosting (Webauftritt der Kommune, reine Informationsdarstellung);
- Betreuung der lokalen IT-Infrastruktur;
- Installation und Betreuung Client-IT in der Kommune durch Beschäftigte der Auftragnehmer vor Ort und durch Fernwartung (Clients, Drucker, Scanner, mobile Geräte usw.);
- Installation und Betreuung lokaler Server;
- Installation und Betreuung der Netzwerk- und Sicherheitskomponenten;
- Einrichtung und/oder Betrieb einer Token-/Smartcard-Verwaltung;
- Rechenzentrumsbetrieb;
- Speicherung / Backup / Archivierung der Daten im Rechenzentrum;
- Verzeichnisdienste;
- Unterstützung mobiles Arbeiten (z. B. Bereitstellung VPN (Virtual Private Network), Remote Desktop (RDP), Telefonsoftware, Tools für Videokonferenzen usw.);
- Betrieb Groupware (E-Mail, Kalender, Videokonferenz, Wiki, usw.);
- Betrieb Fachanwendungen (auch als Webanwendung);
- durch Auftragnehmer entwickelt;
- oder zugekauft/gemietet.

In diesem Zusammenhang müssen auch die unterschiedlichen Auslagerungsszenarien „in die Cloud“ betrachtet werden. Hier gibt es unterschiedliche Auslagerungsszenarien, die im Cloud-Jargon IaaS (Infrastructure as a Service – Bereitstellung von Rechenzentrumsressourcen wie Server, Speicher, Betriebssystem), PaaS (Platform as a Service – Bereitstellung von Infrastruktur und Software) und SaaS (Software as a Service – Bereitstellung von Applikationen mit Zugriff) genannt werden. Für Kommunen können alle denkbaren Szenarien der Cloud interessant sein. Allerdings entstehen mit der Auslagerung in die Cloud unter Umständen weitere Herausforderungen durch Cloud-spezifische Aspekte wie die Verteilung auf mehrere Rechenzentren, deren Standorte und Beschäftigte, die unter Umständen weltweit verteilt sein können, den Betrieb durch eine Firma außerhalb des Geltungsbereichs der Datenschutz-Grundverordnung usw. Hierdurch ergeben sich unter Umständen weitere rechtliche und technische Herausforderungen. **Diese sind nicht Gegenstand des aktuellen Dokuments** und es bedarf einer ausführlichen Risikoabwägung durch die Kommune.

Für derartige Konstellationen kann auf die Ausführungen in den Tätigkeitsberichten des Bayerischen Landesbeauftragten für den Datenschutz (etwa im 28. Tätigkeitsbericht unter Nr. 14.2) hingewiesen werden.[8] Diese Fundstellen beziehen sich zwar im Wesentlichen auf den Zeitraum vor Inkrafttreten der Datenschutz-Grundverordnung, können möglicherweise

[8] Internet: https://www.datenschutz-bayern.de, Rubrik „Tätigkeitsberichte“.

dennoch bei der Bewertung, ob eine Auslagerung in die Cloud zielführend ist, hilfreich sein. Zusätzlich ist das Urteil des Europäischen Gerichtshofes vom 16. Juli 2020, C-311/18, „Schrems-II-Urteil“ zu beachten.[9]. Zudem sollten bei der Nutzung von Diensten aus der Cloud immer beachtet werden, dass ein angemessener Malware-Schutz notwendig ist. Die Beachtung des Cloud Computing Compliance Criteria Catalogue des BSI (BSI C5) wird dringend empfohlen. Da dieser Katalog auch Punkte enthält, welche Bedeutung für die aktuell betrachteten Auslagerungsszenarien haben, wird er bereits zum gegenwärtigen Zeitpunkt unter Nr. 3 behandelt.

Das **aktuelle Dokument** legt den Fokus eher auf die Nutzung von Rechenzentrumsleistungen und den Betrieb von Fachverfahren, aber auch für die anderen genannten Auslagerungsszenarien gibt es Hinweise und Anforderungen, die zu beachten sind.

2.4.3 Allgemeine technisch-organisatorische Anforderungen an die Kommunen

Unabhängig von einem Outsourcing sollen **Kommunen** immer die nachfolgenden allgemeinen Regelwerke beachten:

- Bei der Grundsicherung der eingesetzten Informationstechnik ist ein angemessenes IT-Sicherheitsniveau und ein Informationssicherheitskonzept im Sinn von Art. 11 Abs. 1 Satz 2 BayEGovG erforderlich. Dieses kann für kleine und mittlere Kommunen durch das Siegel „Kommunale IT-Sicherheit“ des Landesamts für Sicherheit in der Informationstechnik (LSI), durch den Standard VdS 10000 oder ISIS12, bei größeren Kommunen durch Einführung eines der üblichen ISMS-Standards (ISIS12, ISO 27001, vorzugswürdig in der Ausprägung des BSI IT-Grundschutz) erreicht werden. Für Gemeinden gibt es die Möglichkeit über ein kommunales Behördennetz (KomBN) eines Landratsamtes Zugang zum Behördennetz zu erlangen. Dabei gelten die sicherheitstechnischen Anschlussbedingungen an das Bayerische Behördennetz in der Teilnehmergruppe 2 und ggf. die (Muster-)Anschlussbedingungen an kommunale Behördennetze. Generell wird allen Kommunen empfohlen, sich an den IT-Sicherheitsrichtlinien für die Bayerische Staatsverwaltung zu orientieren.
- Zum sicheren Einsatz von Windows 10-Systemen wird eine Orientierung am entsprechenden IKT-Leitfaden empfohlen. Dieser ist für die an das Bayerische Behördennetz angeschlossenen Stellen über den Link https://lsi.bybn.de/ikt/index.php abrufbar. Im Übrigen wird auf die Bezugsmöglichkeiten direkt beim Landesamt für Sicherheit in der Informationstechnik verwiesen.

Zusätzlich zu diesen Basisanforderungen an die IT-Sicherheit in den oben genannten Regelwerken werden für das IT-Outsourcing von Kommunen weitere Anforderungen aufgestellt. Ein **Dienstleister**, der für eine Kommune tätig wird, muss neben den für die Kommunen geltenden Regelwerken je nach Szenario der Auslagerung weitere Anforderungen erfüllen.

[9] Siehe hierzu auch meine Pressemitteilung vom 29. Februar 2020, abrufbar auf, https://www.datenschutz-bayern.de, Rubrik „Presse – Archiv“.

2.4.4 Anforderungen an IT-Dienstleister

Im Folgenden werden Anforderungen an **IT-Dienstleister** gelistet, die als besonders erwähnenswert gesehen werden. Diese Aufzählung ist **nicht abschließend**. Die Anforderungen beziehen sich hauptsächlich – aber nicht ausschließlich – auf das Szenario **Rechenzentrumsbetrieb** für Kommunen.

Diese Anforderungen sind gegliedert nach den Informationssicherheitszielen Verfügbarkeit, Vertraulichkeit und Integrität, sowie den Anforderungen an die Rechenschaftspflichten nach Art. 5 Abs. 2 DSGVO. Einige der Anforderungen gelten bereits bei normalem Schutzbedarf der Daten, bei hohem Schutzbedarf sind daneben auch die erhöhten Anforderungen für hohen Schutzbedarf zu beachten. Gekennzeichnet wird dies bei jeder Anforderung durch **(H)** = bei hohem Schutzbedarf und **(N)** = für normalen Schutzbedarf.

2.4.4.1 Verfügbarkeit

A.1 Physischer Schutz der Gebäude, Räume und Rechner und Zugangssicherung zur Sicherstellung der Verfügbarkeit

Der IT-Dienstleister hat einen physischen Schutz der Gebäude, Räume und Rechner nach IT-Grundschutz des BSI zu gewährleisten. **(N)**

A.2 Wiederherstellbarkeit und Ausfallsicherheit

Die Wiederherstellbarkeit der Systeme sollte gewährleistet sein. Zum Thema Ausfallsicherheit sind u.a. die Szenarien Serverausfall beim Dienstleister **(N)**, Ausfall der LAN-Anbindung zum Dienstleister **(H)** und Insolvenz des Dienstleisters zu berücksichtigen **(H)**. In einem SLA (Service Level-Agreement) sollten Punkte wie Terminierung von Wartungsfenstern, die Reaktions- und Behebungszeiten in einem Störfall und auch die Erreichbarkeit außerhalb normaler Geschäftszeiten vertraglich festgelegt werden **(N)**.

A.3 Patchmanagement

Der Dienstleister verpflichtet sich vorliegende Patches, vor allem die mit sicherheitstechnischem Bezug, unverzüglich einzuspielen. Eine vorhergehende Beurteilung auf einem Testsystem wird angeraten. Bei Fachverfahren sollte die Freigabe durch den Hersteller abgewartet werden. Sollte der Dienstleister gleichzeitig Hersteller des Fachverfahrens sein, müssen vertragliche Vereinbarungen über das zeitnahe Einspielen der Patches getroffen werden.

2.4.4.2 Vertraulichkeit

A.4 Trennung der IT-Dienstleistungen

Betreibt der Dienstleister auch Verfahren für andere Kunden aus dem öffentlichen oder nichtöffentlichen Bereich, so sollte eine technische wie organisatorische Trennung erfolgen. Mindestens sollte die kommunale IT auf eigenen physischen oder virtuellen Servern betrieben werden. Es ist in jedem Fall sicher zu stellen, dass weder ein versehentlicher noch anderer ein

unbefugter Zugriff durch einen anderen Kunden erfolgen kann. Die Maßnahmen hierfür sind im IT-Sicherheitskonzept aufzuführen. **(H)**

A.5 Mandantentrennung

Werden mehrere Kommunen beim gleichen IT-Dienstleister betreut, so ist auf eine strikte Mandantentrennung zu achten **(N)**.

A.6 Datenverschlüsselung

- Die Datenübertragung vom und zum Dienstleister hat immer, das heißt auch für normalen Schutzbedarf, verschlüsselt zu erfolgen (bevorzugt über eigene, in der Hoheit der Kommune stehende Leitungswege oder bei öffentlichen Netzen über ein VPN (IPSec, SSL/TLS, entsprechen den Vorgaben der BSI TR-02102-2). **(N)**
- Falls eine Datenkategorie einem hohen Schutzbedarf unterliegt bzw. es rechtlich partiell erforderlich macht, dass der Dienstleister keinesfalls Kenntnis von den personenbezogenen Daten erlangen darf, ist sicherzustellen, dass
  - diese Daten ausschließlich verschlüsselt beim Auftragnehmer gespeichert werden. Sollte eine Anwendung nicht mit einer verschlüsselten Datenbasis arbeiten können, sollten andere Maßnahmen getroffen werden, um eine unbefugte Kenntnisnahme zu verhindern.
  - die Hoheit über die Schlüssel bei der Kommune verbleibt (z. B. Hardware Security Modul).

  (H)

A.7 Sicherstellung der Vertraulichkeit bei Backup und Datenarchivierung

- Backup und Datenarchivierung sollten getrennt für jede Kommune erfolgen, so dass eine Löschung oder Aussonderung bzw. Rückgabe der Daten problemlos möglich ist. **(N)**
- Backup und Archivierung sollten verschlüsselt erfolgen **(N)**, ist ein hoher Schutzbedarf festgestellt worden, so muss diese verschlüsselt erfolgen **(H)**.
- Es sollten offline Backups vorgehalten werden **(N)**
- Für hohen Schutzbedarf gilt weiterhin:
- Der Schlüssel der Datenarchivierung darf nach dem Vorgang der Archivierung ausschließlich der Kommune vorliegen.
- Der Schlüssel für das verschlüsselte Backup ist regelmäßig zu wechseln und darf dem Dienstleister nur so lange vorliegen, wie das Backup für ein schnelles Wiedereinspielen zur Verfügung stehen muss.

(H)

A.8 Zugänge und Berechtigungen

- Zugänge und Berechtigungen für Beschäftigte der Kommune sowohl auf Daten wie auch auf Applikationen sind üblicherweise durch einen Beschäftigten der Kommune nach einem von der Kommune festzulegenden Identitäts- und Berechtigungsmanagement nach dem Minimalprinzip zu vergeben. Die Vergabe kann alternativ an den Dienstleister delegiert werden. Hierfür ist in einem formalisierten Verfahren eindeutig mit dem Dienstleister zu kommunizieren. Die Weisung und deren Umsetzung sind jeweils zu protokollieren. **(N)**
- Es sollte ein ausführliches Berechtigungskonzept vorhanden sein, in dem ebenfalls festgehalten ist, welche Berechtigungen der IT-Dienstleister bzw. dessen Beschäftigte für die Administration und weiteren notwendigen Zugriffe erhalten sollen. **(N)**
- Administratoren des IT-Dienstleisters sollten unter personalisierten Zugängen arbeiten, um in den Protokollen Zugriffe personenspezifisch nachvollziehen zu können. **(N)** Speziell für Ordnungswidrigkeitenverfahren ergeben sich die Anforderungen an die Protokollierung aus § 76 BDSG (in Verbindung mit § 46 Abs. 1 OWiG, § 500 StPO). **(H)**
- Ebenfalls sollte es ein Konzept zum Zugangs- und Berechtigungsentzug bzw. zur Stilllegung von Zugängen und Berechtigungen geben. Hier sind insbesondere die Szenarien Tätigkeitswechsel, Ausscheiden und längere Abwesenheit zu beachten. Der Dienstleister legt ein solches Konzept für seine Beschäftigten vor. **(N)**

A.9 Fremd- und Fernwartung

- Bei der Fremd- und Fernwartung ist darauf zu achten, dass kein unnötiger Zugriff auf personenbezogene Daten durch Beschäftigte des Dienstleisters möglich ist bzw. die Möglichkeit der Kenntnisnahme zu minimieren ist. Hierbei sind die in den Tätigkeitsberichten des Bayerischen Landesbeauftragten für den Datenschutz beschriebenen Sicherheitsmaßnahmen zu beachten (z. B. 20. Tätigkeitsbericht Nr. 17.1.9, 18. Tätigkeitsbericht, 3.3.4). **(N)**
- Bei lokaler Wartung durch Fremdpersonal sind in einem Logbuch Zeitpunkt, Ursache der Wartung und Name dessen, der die Wartung durchführt, festzuhalten. Schließlich sollte die Wartung und Fernwartung nur dann durchgeführt werden, wenn sichergestellt ist, dass ausreichender eigener Sachverstand für die Beurteilung der externen Aktivitäten vorhanden ist und diese überwacht werden. **(N)**
- Der Zugriff sollte lediglich innerhalb des beabsichtigten Wartungsfensters möglich sein. **(N)**
- Darüber hinaus muss der Zugriff über eine verschlüsselte Verbindung erfolgen. **(N)**

A.10 Protokollierung zur Sicherstellung der Vertraulichkeit

- Um unberechtigte Zugriffe durch Angreifer, Administratoren des Dienstleisters und Beschäftigte der Kommune feststellen zu können, ist eine umfangreiche geeignete Protokollierung von Zugriffen und Aktivitäten durchzuführen. **(N)**

- Die Protokolle sollten durch die Verantwortlichen oder von ihm beauftragte unabhängige Experten regelmäßig (anlassbezogen und anlasslos) soweit angezeigt im Vier-Augen-Prinzip ausgewertet werden. Dazu sind sie so zu gestalten, dass eine effektive Überprüfung möglich ist. **(N)**
- Der Einsatz eines zentralen Log-Servers wird angeraten. **(N)**

2.4.4.3 Integrität

A.11 Protokollierung zur Sicherstellung der Integrität

- Die Zwangsläufigkeit und damit die Vollständigkeit der Protokolle sollte gewährleistet werden. **(H)**
- Das Gleiche gilt für die Manipulationssicherheit der Einträge in den Protokolldateien. **(H)**

Die vollständige Protokollierung sorgt für eine Nachvollziehbarkeit der Geschäftsvorfälle und Zugriffe und damit für Revisionssicherheit. **(H)**

2.4.4.4 Rechenschaftspflichten

A.12 Zertifizierungen

Derzeit sind weder Datenschutzzertifizierungen nach Art. 42 DSGVO noch genehmigten Verhaltensregeln nach Art. 41 DSGVO, die eine Alternative zur Zertifizierung darstellen könnten, verfügbar.

Aktuell kann bei der Bewertung eines Dienstleisters auf Grund von Zertifizierungen nur auf Sicherheitszertifizierungen zurückgegriffen werden.

Für Rechenzentrumsleistungen des **IT-Dienstleister** ist üblicherweise eine Zertifizierung nach ISO 27001 zielführend. Eine ISO 27001-Zertifizierung kann anhand des Regelwerks zum IT-Grundschutz des BSI durchgeführt werden, dies ist allerdings nicht verpflichtend. Der Vorteil einer ISO 27001-Zertifizierung auf Basis von IT-Grundschutz ist das zugrundeliegende strukturierte Vorgehen, das mit dem IT-Grundschutz-Katalog vorgegeben ist. Der Dienstleister weist mit der Zertifizierung nach ISO 27001 zumeist seine Eignung als Rechenzentrum für die Verarbeitung von Datenkategorien für einen normalen Schutzbedarf nach. Allerdings ist in jeden Fall der Anwendungsbereich der Zertifizierung zu überprüfen. Das BSI führt beispielsweise eine Liste der ausgestellten Zertifikate inklusive des Untersuchungsgegenstandes[10]. Dieser muss alle an den Auftragsverarbeiter übertragenen Aufgaben, Dienste und Hilfstätigkeiten umfassen. Anhand des Untersuchungsgegenstandes des Zertifikats ist zu prüfen, ob weitere Anforderungen aus diesem Katalog vertraglich vereinbart und umgesetzt werden müssen. Für ISO 27001 Zertifizierungen auf Basis von IT-Grundschutz des BSI dient Nr. 3 als Hilfestellung hierfür.

Zu beachten: Ggf. können Angebote den unzutreffenden/irreführenden Eindruck erwecken, dass ein Zertifikat eines Unterauftragnehmers sich auf das komplette Angebot erstreckt. Ein

[10] Für BSI-Zertifizierungen kann der Untersuchungsgegenstand anhand der Zertifikatsnummer auf den Seiten des BSI (https://www.bsi.bund.de) eingesehen werden.

Beispiel hierfür wäre die Nutzung von angemieteten Räumlichkeiten mit einer professionell betriebenen zertifizierten technischen Infrastruktur (sog. Colocation- oder ServerHousing-Leistungen) zur Erbringung weiterer Leistungen wie z. B. Betrieb von Server-Systemen, Netzwerk-Komponenten und Peripheriegeräten, Firewall, automatisierten Verfahren, Datenbanken, Datensicherung sowie IT-Support. Der genaue Umfang der vorgelegten Zertifikate ist daher stets detailliert in den Blick zu nehmen.

Kann der Auftragnehmer keine ausreichende Zertifizierung nachweisen, ist ein ausführliches Sicherheitskonzept vorzulegen, dass durch die Kommune oder einen externen Experten geprüft werden sollte. Üblicherweise legt ein Auftragnehmer ein Sicherheitskonzept für einen normalen Schutzbedarf vor.

In jeden Fall ist somit zu prüfen, ob weitere Anforderungen auf Grund des datenschutzrechtlichen Schutzbedarfs der Daten erfüllt sein müssen.

A.13 IT-Sicherheits- und Datenschutzvorfälle

Der Dienstleister führt eine umfassende Sicherheitsprotokollierung an allen relevanten Komponenten durch und wertet diese in Bezug auf mögliche Angriffe aus und übernimmt Abhilfemaßnahmen. IT-Sicherheits- und Datenschutzvorfälle sind der Kommune unverzüglich zu melden. Für die Abläufe bei Datenschutzverstößen und deren Meldung nach Art. 33 DSGVO (bzw. im Ordnungswidrigkeitenverfahren nach § 65 BDSG in Verbindung mit § 46 Abs. 1 OWiG, § 500 StPO) ist eine konkrete Vorgehensweise **vertraglich festzulegen**.

A.14 Audits / Kontrollen / Zugang

Audits, Testate und Kontrollen dienen der Überprüfung, ob Anforderungen bzw. Richtlinien eingehalten werden. **Audits** und **Testate** werden von besonders geschulten Auditoren durchgeführt. Im Rahmen einer Zertifizierung werden üblicherweise Zertifizierungsaudits und Überwachungsaudits von akkreditierten Auditoren durchgeführt. Der Auditbericht wird durch eine unabhängige Zertifizierungsstelle überprüft. Diese stellt das **Zertifikat** aus. Zertifizierungsaudits dienen der Erstzertifizierung und der Rezertifizierung (z. B. bei ISO 27001 auf Basis von IT-Grundschutz nach drei Jahren), Überwachungsaudits werden üblicherweise jährlich durchgeführt und dienen der Überprüfung der weiteren Entwicklung des Zertifizierungsgegenstands. Ein Testat wird indessen durch den Auditor ausgestellt. Eine unabhängige Zertifizierungsstelle ist hier nicht beteiligt. Für **Kontrollen** gibt es keine formalen Vorgaben. In einer Kontrolle bzw. auch Inspektion nach Art. 28 DSGVO überprüft der Auftraggeber die Einhaltung der Pflichten des Auftragnehmers.

Die Kommune sollte durch eigenes qualifiziertes Personal oder Sachverständige regelmäßig Kontrollen beim Auftragsverarbeiter durchführen. Hierfür ist der Zugang zu den Räumen zu gewähren. Ebenfalls sollten sie zu den Beschäftigten des Dienstleisters, die für die Administration und Betreuung der kommunalen IT zuständig sind, Zugang haben. Der behördliche Datenschutzbeauftragte und der Informationssicherheitsbeauftragte sind zu beteiligen. Dem kann die Kommune auch dadurch nachkommen, dass sie sich vom Dienstleister bereits dort durchgeführte aktuelle Audits bescheinigen lässt.

Für den Fall, dass der Dienstleister nach ISO 27001 zertifiziert ist, kann die Kommune in der Regel auf eigene Kontrollen verzichten. Dies ist dadurch begründet, dass ein akkreditierter Auditor das Erstaudit sowie nach maximal drei Jahren ein Rezertifizierungsaudit und ggf. zusätzlich jährliche Überwachungsaudits durchführt. Die Kommune muss in diesem Fall lediglich überprüfen, ob eine Rezertifizierung durchgeführt wurde, die zwischenzeitlich auch nicht entfallen ist.

Hinweis: Eine Zertifizierung nach ISO 27001 reduziert unter Umständen die Kontrollpflicht beim Auftragnehmer, befreit aber nicht von der sorgfältigen Auswahl des Dienstleisters mit Überprüfung, ob der Untersuchungsgegenstand der Zertifizierung anwendbar ist und ggf. weitere technische Anforderungen aus diesem Anforderungskatalog vertraglich zu vereinbaren sind.

A.15 Penetrationstests

Der Dienstleister lässt regelmäßig Rechenzentrumsinfrastruktur- und Serverkomponenten mittels Penetrationstests überprüfen. Bietet der Dienstleister das Hosting von Fachanwendungen an, so sind auch hier regelmäßige Penetrationstests notwendig. Diese können sich auf die in der Verantwortung des Betreibers liegenden Komponenten beschränken. So sind generell Fehlkonfigurationen (beispielsweise des Webservers) in der Verantwortung des Betreibers, Fehler im Softwareprodukt sind nur in der Verantwortung des Betreibers, wenn er auch der Entwickler des Produkts ist.

Einen Nachweis erbringt der Dienstleister mindestens alle drei Jahre.

2.4.5 Zwingend bei der Kommune verbleibende Kompetenzen

Um ihrer Rolle als datenschutzrechtlich Verantwortlicher gerecht zu werden, benötigt die Kommune auch im Falle eines IT-Outsourcings Mitarbeiter, die für IT-Fragen hinreichend kompetent sind (vgl. Nr. 2.2.5). Eine Vertretung sollte sichergestellt sein. Erforderlichenfalls sind die Möglichkeiten kommunaler Zusammenarbeit im Rahmen des hierfür zur Verfügung stehenden Rechtsrahmens zu nutzen. Die folgenden Aufgaben sollten unter der Hoheit der IT-Beauftragten (gegebenenfalls unter Einschaltung unabhängiger externer Sachverständiger) mindestens übernommen werden können:

- Schriftliche Vereinbarung der Aufgaben von Auftraggeber und Auftragnehmer zu technischen Fragen;
- Erteilung fachlich versierter Weisungen;
- regelmäßige Überprüfung der Protokollierung;
- regelmäßige Kontrollen bzw. fachlich versierte Auswertung der Auditberichte, falls ein externer Prüfer hinzugezogen wurde oder sich die Gemeinde Bescheinigungen des Dienstleisters vorlegen lässt;
- Koordinierung verschiedener Auftragsverarbeiter und externer Berater sowie unabhängiger Prüfer;

- Vergabe der Accounts und Berechtigungen nach dem zum Einsatz kommenden Berechtigungskonzept – entweder durch den IT-Beauftragten selbst oder auf ausdrückliche Weisung des IT-Beauftragten;
- Verwaltung der kryptographischen Schlüssel für verschlüsselte Backups/Archive;
- Risikoabschätzung, Beteiligung an Datenschutz-Folgenabschätzung.
- Verantwortung über die Überwachung der Einhaltung der IKT-Sicherheitsrichtlinien soweit Betroffenheit vorliegt und anwendbar – insbesondere Verantwortung über die Einhaltung der sicherheitstechnischen Anschlussbedingungen an das Bayerische Behördennetz in der Teilnehmergruppe 2 (z. B. Kommunen)

3 Anhang: Praxishilfen

In diesem Anhang wird für zwei praxisrelevante Auslagerungsszenarien aufgezeigt, welche Anforderungen durch die gängigen angebotenen Sicherheitszertifikate abgedeckt werden, bzw. in welchen Fällen eine zusätzliche, weitergehende Prüfung durch die Gemeinde erforderlich ist. Der Anhang ist als „wachsendes/lebendes" Dokument gedacht und wird daher angepasst werden, falls neue relevante Zertifizierungen vorliegen.

3.1 Berücksichtigte Zertifikate, Zertifizierungen, Testate, Standards

3.1.1 ISO/IEC 27001

Häufige Zertifizierung für den Rechenzentrumsbetrieb für normalen Schutzbedarf. Weiteres siehe Nr. 2.4.4.4 A.12.

Anmerkung: Der IT-Grundschutz des BSI verweist im Baustein Datenschutz auf das Standarddatenschutzmodell (SDM). Da die Bausteine des SDM noch nicht alle verfügbar sind, ist eine komplette Umsetzung des SDMs zum Zeitpunkt der Zertifizierung nicht möglich, die Umsetzung einzelner bereits vorhandener Bausteine sollte vor Vertragsabschluss geprüft werden.

3.1.2 BSI Cloud Computing Compliance Criteria Catalogue (kurz: BSI C5)

Ein Kriterienkatalog des BSI für den Betrieb von Cloud-Diensten.

Die Erfüllung der Kriterien kann beispielsweise durch Wirtschafts- oder andere geeignete Prüfer testiert und somit gegenüber Kunden nachgewiesen werden. Diese Prüfer werden in diesem Fall direkt vom Cloud-Anbieter beauftragt.

Der Kunde des Cloud-Anbieters sollte die Einhaltung der Kriterien aus diesem Kriterienkatalog als einen wesentlichen Bestandteil seiner Beauftragung ansehen und dies auch mit dem Anbieter vereinbaren. Dies gilt insbesondere für den Fall, wenn die Zusatzkriterien durch den Cloud-Anbieter erfüllt werden sollen. Ferner sollte der potenzielle Cloud-Kunde seine Entscheidung nicht nur auf eine vorhandene, aktuelle Berichterstattung nach diesem Kriterienkatalog gründen (unabhängig, ob diese sich auf die Basis- oder Zusatzkriterien bezieht), sondern sollte sich die Berichterstattung des (Wirtschafts-)prüfers vom Cloud-Anbieter regelmäßig vorlegen lassen und diesen für seinen Anwendungsfall bewerten.

3.1.3 BSI-Standard Sicheres Bereitstellen von Web-Angeboten (ISi-Webserver)

Das BSI hat Standards zur Internet-Sicherheit (ISi-Reihe) herausgegeben. Hierunter befindet sich der Standard „Sicheres Bereitstellen von Web-Angeboten (ISi-Webserver)“. Der Standard ist als Hilfestellung für den Betreiber zu betrachten.

3.2 Überprüfen des Anforderungskatalogs bei vorhandener Zertifizierung für zwei besonders relevante Varianten

Im Folgenden sollen einige Outsourcing-Varianten mit möglichen Zertifizierungen und den damit verbundenen Erleichterungen bei der Prüfung der Anforderungen für eine Auslagerung von Kommunen dargestellt werden. Diese Aufstellung erhebt keinerlei Anspruch auf Vollständigkeit. Sollten Anbieter weitere Zertifizierungen, Audit-Ergebnisse von Prüfungen oder Selbstauskünfte zur Verfügung stellen, können diese ebenfalls als Hilfsmittel zur Beurteilung der Zuverlässigkeit des Anbieters herangezogen werden.

3.2.1 Webhosting

Das Webhosting wird hier als reine Informationsdarstellung der Kommune betrachtet. Sobald Fachanwendungen über den Webauftritt der Kommune angeboten werden, sollten weitere Sicherheitsanforderungen erfüllt werden.

Auch ein Dienstleister, der den Webauftritt der Kommune betreut, sollte sorgfältig ausgewählt werden. Da hierbei allerdings in der Regel keine sensiblen personenbezogenen Daten verarbeitet werden, sind keine besonderen Anforderungen einzuhalten, die lediglich Kommunen betreffen.

Für Webhosting gibt es derzeit keine direkten Zertifizierungen, allerdings kann eine Zertifizierung nach ISO 27001 das Webhosting umfassen. Hierfür ist anhand der Zertifikatsnummer der Anwendungsbereich des Zertifikats zu prüfen.

Das BSI hat außerdem Standards zur Internet-Sicherheit (ISi-Reihe) herausgegeben. Hierunter befindet sich der Standard „Sicheres Bereitstellen von Web-Angeboten (ISi-Webserver)“. Ein Dienstleister, der sich an diesen Standard hält, ist für das Szenario Webhosting als vertrauenswürdig zu betrachten. Allerdings kann dies nicht durch ein Zertifikat nachgewiesen werden, sondern muss als Selbstauskunft durch den Dienstleister erfolgen. Somit verbleibt die Pflicht zur Prüfung, ob dieser Standard eingehalten wird bei der Kommune.

3.2.2 Rechenzentrumsbetrieb

Rechenzentrumsbetrieb oder auch Hosting ist die Bereitstellung von Hardware, Fachanwendungen und Fachpersonal zur Administration durch einen Auftragnehmer. Im Gegensatz zum

Cloud-Computing werden üblicherweise dezidierte Server in einem festgelegten Rechenzentrum sowie lokal angesiedeltes Servicepersonal (hauptsächlich zur Administration) zur Erbringung der Dienste eingesetzt. Damit werden im Rechenzentrumsbetrieb die üblichen Dienste durch den Auftragnehmer übernommen, die nach Stand der Technik einem normalen Arbeitsplatz zur Verfügung stehen sollen. Hierunter fallen

- die Datenspeicherungen auf einem Datei-Server (NAS), Backup und ggf. Archivierung der Daten,
- die Verzeichnisdienste zur Vergabe von Nutzeraccounts und Berechtigungen
- Dienste zur Unterstützung von mobilem Arbeiten (Einwahl per VPN oder RDP (sichere Einwahl ins Netz der Kommune oder das bay. Behördennetz), Bereitstellung von Telefonsoftware und Tools für Videokonferenz), sowie
- Bereitstellung von Diensten zur Zusammenarbeit (Groupware) wie E-Mail, gemeinsamer Kalender, Wiki, usw.)
- Bereitstellung von Fachanwendungen z. B. als Webanwendung
- Häufig wird mit der Zertifizierung nach ISO 27001 (z. B. auf der Basis von IT-Grundschutz des BSI) ein Rechenzentrumsbetrieb zertifiziert. Es ist allerdings in jedem Fall nicht nur das Vorhandensein der Zertifizierung, sondern auch der Untersuchungsgegenstand und der geprüfte Schutzbedarf zu überprüfen.

3.3 Abdeckung der Anforderungskriterien durch ISO 27001 auf Basis von IT-Grundschutz und BSI C5

Die folgenden Tabellen zeigen, in wie weit ein Dienstleister mit einer Zertifizierung nach ISO 27001 auf Basis von IT-Grundschutz oder einem Testat über die Einhaltung der BSI Cloud Computing Compliance Criteria Catalogue (kurz: BSI C5) die Kriterien des Anforderungskatalogs für den Auslagerungsfall „Rechenzentrum“ erfüllt.

Anhand der Spalten „Kriterium mit Zertifizierung nicht weiter zu betrachten“, „Kriterium benötigt weitere Betrachtung“, „Kriterium auch mit Zertifizierung nicht erfüllt“ kann überblicksartig überprüft werden, welche Anforderungen über die Zertifizierung bzw. die Testaterfüllung hinaus umgesetzt werden sollen bzw. müssen. In Spalte 1 finden sich dann Hinweise, welche (Teil-)Anforderungen noch offen sind.

Die Auswahl der Standards erfolgte nach folgenden Überlegungen:

Eine bereits verbreitete Zertifizierung unter IT-Dienstleistern ist eine Zertifizierung nach ISO 27001 auf Basis von IT-Grundschutz. Die nachfolgende Tabelle zeigt die Differenz zwischen Zielerfüllung des Standards und diesem Anforderungskatalog.

Zunehmend werden Hosting-Angebote auch als Private-Cloud-Angebote konzipiert. Diese sind wie bereits ausgeführt, derzeit nicht direkt Gegenstand dieses Kriterienkatalogs. Gleichwohl ist es durchaus zu befürworten, wenn Anbieter die Einhaltung dieser Kriterien anstreben.

Für Gemeinden liegt der Vorteil eines Dienstleisters, der sich an die BSI C5-Kriterien hält darin, dass weite Teile dieses Anforderungskatalogs abgedeckt sind. Diese Zielerfüllung findet sich in der Tabelle unter Nr. 3.3.2.

3.3.1 ISO 27001 auf Basis von IT-Grundschutz

Grundannahme: Der Untersuchungsgegenstand des Zertifikats beinhaltet den Rechenzentrumsbetrieb, die Bereitstellung von Webanwendungen, sowie die Administrationsarbeitsplätze des Dienstleisters zertifiziert nach ISO 27001 auf Basis von IT-Grundschutz mit Schutzbedarf „normal".

Hinweis: In Klammern findet sich zur vertiefenden Information der jeweilige Baustein des IT-Grundschutz

	Kriterium mit Zertifizierung nicht weiter zu betrachten	Kriterium benötigt weitere Betrachtung	Kriterium auch mit Zertifizierung nicht erfüllt
A.1 physischer Schutz der Gebäude, Räume und Rechner und Zugangssicherung zur Sicherstellung der Verfügbarkeit Die Anforderungen des IT-Grundschutz umfassen den benötigten physischen Schutz. (INF)	✔		
A.2 Wiederherstellbarkeit und Ausfallsicherheit Die Anforderungen des IT-Grundschutz umfassen die notwendigen Maßnahmen zur Wiederherstellbarkeit. (DER.4) **Auch mit Zertifizierung ist zu prüfen:** – Ggf. müssen die Daten und Dienste auf Grund der Notwendigkeit einer hohen Verfügbarkeit in einem Ausfallrechenzentrum redundant verfügbar sein. – bei privatwirtschaftlichen Anbietern ggf. auf Grund von rechtlichen Vorgaben: Maßnahmen zur Absicherung im Insolvenzfall notwendig. – Ein SLA (Service-Level-Agreement) ist abzuschließen.		!	
A.3 Patchmanagement Die Anforderungen des IT-Grundschutz umfassen die notwendigen Maßnahmen für ein ordnungsgemäßes Patchmanagement. (OPS.1.1.3)	✔		

	Kriterium mit Zertifizierung nicht weiter zu betrachten	Kriterium benötigt weitere Betrachtung	Kriterium auch mit Zertifizierung nicht erfüllt
A.4 Trennung der IT-Dienstleistungen Die Anforderungen des IT-Grundschutz umfassen die notwendigen Maßnahmen zur Erstellung und Umsetzung eines Mandantenkonzepts und somit zur Trennung der IT-Dienstleistungen. Das Mandantenkonzept soll laut BIS- Grundschutz dem Auftraggeber vorgelegt werden. (OPS.3.1.A7) **Auch mit Zertifizierung ist zu prüfen:** – Hat der Auftragnehmer auch Kunden aus dem nicht-öffentlichen Bereich, so sollen sich zur Abschottung der Kunden des öffentlichen und nicht-öffentlichen Bereichs Maßnahmen im Mandantenkonzept finden.		!	
A.5 Mandantentrennung Die Anforderungen des IT-Grundschutz umfassen die Mandantentrennung. (OPS.3.1.A7)	✔		
A.6 Datenverschlüsselung Die Anforderungen des IT-Grundschutz umfassen die notwendigen Maßnahmen zur Verschlüsselung der Kommunikationsverbindung. (NET.3.3, OPS.3.1.A8) Auch wenn der IT-Grundschutz Bausteine für ein Verschlüsselungskonzept vorweist, gibt es keine Bausteine, die den Bedarf einer Datenverschlüsselung für Outsourcing-Kunden abdecken, deshalb ist. **Auch mit Zertifizierung zu prüfen:** – Hat eine Datenkategorie einen Schutzbedarf, dass der Auftraggeber keinerlei Kenntnis von den Daten erhalten hat, sind zusätzliche Maßnahmen zu treffen.		!	
A.7 Sicherstellung der Vertraulichkeit bei Backup und Datenarchivierung Die Anforderungen des IT-Grundschutz umfassen die notwendigen Maßnahmen für ein Datensicherungskonzept. (CON.3) **Auch mit Zertifizierung sind folgende Forderungen aus diesem Bereich zu prüfen:** – Eigenständiges Backup und Archivierung für jede Kommune; – Backup und Archivierung je nach Schutzbedarf ggf. verschlüsselt; – Bei hohem Schutzbedarf aus spezialrechtlichen Regelungen: ▪ Schlüsselbesitz bei Archivierung ausschließlich bei der Kommune ▪ Schlüsselbesitz beim Backup nur solange beim Auftragnehmer wie notwendig, regelmäßiger Wechsel.		!	

	Kriterium mit Zertifizierung nicht weiter zu betrachten	Kriterium benötigt weitere Betrachtung	Kriterium auch mit Zertifizierung nicht erfüllt
A.8 Zugänge und Berechtigungen Die Anforderungen des IT-Grundschutz umfassen die notwendigen Maßnahmen für ein Berechtigungskonzept. (ORP.4) **Auch mit Zertifizierung sind folgende Forderungen zu erfüllen:** – Die Kommune sollte zusammen mit dem Anbieter festlegen, wie mit dem Identitäts- und Berechtigungsmanagement für die Beschäftigten der Kommune umgegangen wird. – Vorhanden-Sein von personalisierten Zugängen für die Administratoren des IT-Dienstleisters.		!	
A.9 Fremd- und Fernwartung Die Anforderungen des IT-Grundschutz umfassen die notwendigen Maßnahmen für ein Konzept für die Fernwartung im eigenen Verantwortungsbereich (OPS.1.2.5). Soll der Dienstleister auch die Möglichkeit der Fernwartung der Arbeitsplätze der Kommune haben, so sind mit Zertifizierung die **Folgende Forderungen aus diesem Bereich sind zu prüfen:** – Die Möglichkeit der Kenntnisnahme von personenbezogenen Daten ist zu minimieren. – Es ist ein Logbuch über die Fernwartungen zu führen. – Es ist sicherzustellen, dass die Fernwartung über eine verschlüsselte Verbindung erfolgt.		!	
A.10 Protokollierung zur Sicherstellung der Vertraulichkeit Die Anforderungen des IT-Grundschutz umfassen die notwendigen Maßnahmen für ein Protokollierungskonzept (OPS.1.1.5). Außerdem verweist der IT-Grundschutz im Baustein Datenschutz auf das Standarddatenschutzmodell (SDM). Das SDM enthält den Baustein 43 „Protokollierung". Hieraus sollten die Standardanforderungen und in Abhängigkeit des Schutzbedarfs die Anforderungen mit hohem Schutzbedarf umgesetzt sein. Da die Bausteine des SDM noch nicht alle verfügbar sind, ist eine komplette Umsetzung des SDMs zum Zeitpunkt der Zertifizierung nicht möglich. **In jedem Fall sollte überprüft werden, ob Baustein 43 umgesetzt wurde.**		!	
A.11 Protokollierung zur Sicherstellung der Integrität **siehe A.10.**		!	
A.12 Zertifizierungen n. a.			

	Kriterium mit Zertifizierung nicht weiter zu betrachten	Kriterium benötigt weitere Betrachtung	Kriterium auch mit Zertifizierung nicht erfüllt
A.13 IT-Sicherheits- und Datenschutzvorfälle Die Anforderungen des IT-Grundschutz umfassen die notwendigen Maßnahmen für eine umfassende Protokollierung und Auswertung zu Sicherheitszwecken. (DER.1) Die konkrete Vorgehensweise zur Meldung nach Art. 33 DSGVO ist vertraglich festzulegen.		!	
A.14 Audits / Kontrollen / Zugang Die Zertifizierung nach ISO 27001 auf Basis von IT-Grundschutz muss regelmäßig aktualisiert werden. Die Kommune sollte prüfen, ob die Zertifizierung erneuert wurde. Zu Kontrollen und Zugang durch den Auftraggeber finden sich keine Festlegungen in dieser Zertifizierung, diese sind gesondert zu prüfen.		!	
A.15 Penetrationstests Die Anforderungen des IT-Grundschutz umfassen die notwendigen Maßnahmen für Penetrationstests für Webserver (APP.3.2) und Firewall (NET.3.2). Sowohl die Häufigkeit wie die Ziele von Penetrationstests sollten vertraglich festgelegt werden.		!	

3.3.2 BSI Cloud Computing Compliance Criteria Catalogue (kurz: BSI C5)

Grundannahme: Der Dienstleister erfüllt die C5 des BSI und kann dies auf Grund von Prüfberichten eines Wirtschaftsprüfers nachweisen.

Hinweis: In Klammern findet sich zur vertiefenden Information der jeweilige Bereiche bzw. Kriterien des C5-Katalogs

	Kriterium mit Nachweis für C5 nicht weiter zu betrachten	Kriterium benötigt weitere Betrachtung	Kriterium auch mit Nachweis für C5 nicht erfüllt
A.1 physischer Schutz der Gebäude, Räume und Rechner und Zugangssicherung zur Sicherstellung der Verfügbarkeit C5-Rechenzentren sind nach den C5-Kriterien hochverfügbar, redundant und mit vertraglich festgelegter Ausfallzeit. Keine weitere Prüfung durch die Kommune erforderlich. (Bereich PS)	✔		
A.2 Wiederherstellbarkeit und Ausfallsicherheit C5-Rechenzentren sind nach den C5-Kriterien hochverfügbar, redundant und mit vertraglich festgelegter Ausfallzeit. (Bereich PS) **Auch mit C5-Umsetzung ist zu prüfen:** – Bei privatwirtschaftlichen Anbietern ggf. auf Grund von rechtlichen Vorgaben: Maßnahmen zur Absicherung im Insolvenzfall notwendig.		!	
A.3 Patchmanagement Die C5-Kriterien umfassen die notwendigen Maßnahmen für ein ordnungsgemäßes Patchmanagement. (AM-02, OPS-22, PSS-03, DEV-03)	✔		
A.4 Trennung der IT-Dienstleistungen Eine strikte Trennung aller Mandanten ist laut C5-Kriterien vorgeschrieben. (OPS-24)	✔		
A.5 Mandantentrennung s. o.	✔		
A.6 Datenverschlüsselung Laut C5-Kriterien sind die Kommunikationswege zum Kunden abgesichert (CRY-02) und es gibt Verfahren, um die Kundendaten zu verschlüsseln (CRY-03). **Auch mit C5-Umsetzung ist zu prüfen:** – Hat eine Datenkategorie einen Schutzbedarf, dass der Auftraggeber keinerlei Kenntnis von den Daten erhalten hat, sind zusätzliche Maßnahmen zu vereinbaren.		!	

	Kriterium mit Nachweis für C5 nicht weiter zu betrachten	Kriterium benötigt weitere Betrachtung	Kriterium auch mit Nachweis für C5 nicht erfüllt
A.7 Sicherstellung der Vertraulichkeit bei Backup und Datenarchivierung Laut C5-Kriterien werden Backups verschlüsselt. (OPS-06) **Auch mit C5-Umsetzung ist zu prüfen:** – Bei hohem Schutzbedarf aus spezialrechtlichen Regelungen: – Schlüsselbesitz bei Archivierung ausschließlich bei der Kommune – Schlüsselbesitz beim Backup nur solange beim Auftragnehmer wie notwendig, regelmäßiger Wechsel.		!	
A.8 Zugänge und Berechtigungen Laut C5-Kriterien stellt der Cloud-Anbieter den Kunden die Möglichkeit einer Verwaltung von Zugangs- und Zugriffsberechtigungen zur Verfügung (PSS-08). Für Zugangs- und Zugriffsberechtigungen der Beschäftigten des Dienstleisters werden in den C5-Kriterien ebenfalls ausreichende Anforderungen definiert (Bereich IDM) **Auch mit C5-Umsetzung sind folgende Forderungen zu erfüllen:** Vorhanden-Sein von personalisierten Zugängen für die Administratoren des IT-Dienstleisters.		!	
A.9 Fremd- und Fernwartung **Die C5-Kriterien umfassen keine Vorgaben zur Fernwartung, da dieses Szenario nicht zum üblichen Angebot eines Cloud-Anbieters gehört. Soll der Auftragnehmer Fernwartung durchführen, sind alle Kriterien der Fernwartung zu prüfen.**			✗
A.10 Protokollierung zur Sicherstellung der Vertraulichkeit Die C5-Kriterien geben die Möglichkeit Schutzziele zu definieren (OPS-12). Es ist zu prüfen, ob in den Schutzzielen des Auftragnehmers die Überprüfung unberechtigter Zugriffe durch Angreifer, Administratoren, Beschäftigte der Kommune oder andere Externe aufgenommen ist. Zudem ist zu vereinbaren, dass der Anbieter die kundenspezifische Protokollierung zur Verfügung stellt. (OPS-14)		!	
A.11 Protokollierung zur Sicherstellung der Integrität Die C5-Kritrien erfüllen alle Anforderungen aus diesem Punkt. (OPS-14, OPS-15, OPS-16)	✓		
A.12 Zertifizierungen Für die Einhaltung der C5-Kriterien gibt es derzeit keine Zertifizierungsmöglichkeit.			

	Kriterium mit Nachweis für C5 nicht weiter zu betrachten	Kriterium benötigt weitere Betrachtung	Kriterium auch mit Nachweis für C5 nicht erfüllt
A.13 IT-Sicherheits- und Datenschutzvorfälle Die C5-Kriterien definieren Anforderungen an eine Protokollierung und Überwachung und den Umgang mit Schwachstellen fest. (OPS-1*) Zur Einbindung des Kunden bei Störungen werden ebenfalls Maßnahmen definiert (OPS-21). **Für den Umgang mit Datenschutzvorfällen und zur konkreten Vorgehensweise zur Meldung nach Art. 33 DSGVO sind zusätzlich vertragliche Regelungen zu treffen.**		!	
A.14 Audits / Kontrollen / Zugang Das Einhalten der C5-Kriterien kann beispielsweise durch einen Wirtschaftsprüfer geprüft werden. Die Ergebnisberichte hierzu sollte sich die Kommune regelmäßig vorlegen lassen. **Zu Kontrollen und Zugang durch den Auftraggeber finden sich keine Festlegungen in den C5-Kriterien. Diese sind gesondert zu prüfen.**		!	
A.15 Penetrationstests In den C5-Kriterien werden Anforderungen an mindestens jährlich durchzuführende Penetrationstest definiert. (OPS-19)	✔		

4 Anhang: Ablaufschema

IT-Outsourcing geplant?

- Vorüberlegung: siehe insbesondere meine Orientierungshilfe „Auftragsverarbeitung“ (Fn. 5) unter Nr.1 c).
- Die Kommune kann nicht alles aus der Hand geben, weil sie datenschutzrechtlich Verantwortlicher ist: Es entspricht dem Wesen der Auftragsverarbeitung, dass der Verantwortliche Weisungen erteilt und deren Einhaltung kontrolliert.
- Aufgaben, die die Kommune weiterhin erfüllen muss (Nr. 2.4.5).
- Schriftliche Vereinbarung der Aufgaben von Auftraggeber und Auftragnehmer zu technischen Fragen.
- Erteilung fachlich versierter Weisungen (Nr. 2.2.5).
- Regelmäßige Überprüfung der Protokollierung.
- Regelmäßige Kontrollen.
- Koordinierung verschiedener Auftragsverarbeiter und externer Berater sowie unabhängiger Prüfer.
- Vergabe der Accounts und Berechtigungen nach dem zum Einsatz kommenden Berechtigungskonzept – entweder durch den IT-Beauftragten selbst oder auf ausdrückliche Weisung des IT-Beauftragten.
- Verwaltung der kryptographischen Schlüssel für verschlüsselte Backups/Archive.
- Risikoabschätzung, Beteiligung an DSFA.
- Verantwortung über die Überwachung der Einhaltung der IKT-Sicherheitsrichtlinien soweit Betroffenheit vorliegt und anwendbar – insbesondere Verantwortung über die Einhaltung der sicherheitstechnischen Anschlussbedingungen an das Bayerische Behördennetz in der Teilnehmergruppe 2 (z. B. Kommunen).

Was soll ausgelagert werden?

- Siehe Auslagerungsszenarien unter Nr. 2.4.2.

Welche Daten sind davon betroffen?

- Personenbezogene Daten? – Datenschutzrechtliche Bestimmungen zu beachten, insbesondere DSGVO.
- Besondere Kategorien von Daten? – Dann zusätzlich spezialgesetzliche Regelungen zu beachten, z. B.:
  - Meldedaten, Nr. 2.1.1,
  - Steuerdaten, Nr. 2.1.2,
  - Sozialdaten, Nr. 2.1.3,
  - Personalaktendaten, Nr. 2.1.4,
  - Daten im Zusammenhang mit der Verfolgung von Ordnungswidrigkeiten, Nr. 2.1.5.

Entscheidung für Outsourcing gefallen – was ist zu beachten?

- Auswahl eines Dienstleisters (in Nr. 2.2.3 werden verschiedene Konstellationen aufgezeigt).

  Bei der Auswahl ist insbesondere Art. 28 Abs. 1 DSGVO zu beachten.

  Dabei ist auf Zertifizierung zur IT-Sicherheit, ununterbrochenen und zuverlässigen Betrieb der IT, qualifiziertes Personal und kompetente Ansprechpartner für Datenschutz und IT-Sicherheit zu achten (Nr. 2.2.1).
- Es muss mit dem Auftragsverarbeiter ein Vertrag abgeschlossen werden. Der Inhalt ergibt sich aus:
  - Art. 28 Abs. 3 DSGVO (Nr. 2.2.2–Nr. 2.2.8)
  - Haushaltsrechtlichen Grundsätzen (Nr. 2.3)
  - Technisch-organisatorische Kriterien (Nr. 2.4):
    - In einer **Risikoanalyse** ist zu ermitteln, welche Kriterien konkret einzuhalten sind. Die Vorgehensweise ergibt sich aus meiner Orientierungshilfe „Datenschutz-Folgenabschätzung“ (Fn. 7).

      Vorab ist der jeweilige Schutzbedarf der Daten festzustellen.
    - Maßnahmen, die zu treffen sind um das Risiko zu minimieren Zur Sicherstellung der **Verfügbarkeit** (Nr. 2.4.4.1), **Vertraulichkeit** (Nr. 2.4.4.2) und **Integrität** (Nr. 2.4.4.3)
- Diese Anforderungen sind im **Vertrag** festzuhalten.