Landesamt für Sicherheit in der Informationstechnik

Leitfaden „Phasen eines Beschaffungsvorhabens“

Für staatliche und kommunale Organisationen sowie Betreiber von kritischen Infrastrukturen

DOKUMENTINFORMATIONEN

Erstellt am:	07.11.2022		
Version	1.0		
Seitenanzahl	13	© 2022 Landesamt für Sicherheit in der Informationstechnik	**TLP:GREEN**

INHALT

Vorwort

Informationssicherheit ist mehr denn je ein wichtiger Bestandteil für alle Organisationen, die Informationstechnologie (IT) einsetzen. Dabei ist sie nicht nur für interne Prozesse von besonderer Bedeutung, sondern auch ein bedeutender Faktor, wenn IT-bezogene Aufgaben von externen Dienstleistern übernommen werden. Eine sogenannte Auslagerung von Geschäftsprozessen kann für Organisationen Vorteile, aber auch gewisse Risiken und Gefahren mit sich bringen und Rückwirkungen auf die Informationssicherheit haben.

Das vorliegende Dokument dient als Hilfestellung. Es betrachtet den informationssicherheitstechnischen Aspekt, wenn staatliche und kommunale Organisationen sowie Betreiber von kritischen Infrastrukturen Softwareprodukte, IT-Hardware oder IT-Dienstleistungen beschaffen möchten.

Zur besseren Abgrenzung ist das Thema in sieben Phasen unterteilt, die jeweils näher beschrieben werden. Die zu jeder Phase im folgenden Dokument aufgeführten, nicht abschließenden Leitfragen weisen dabei auf Gedanken hin, die in der entsprechenden Phase beantwortet werden sollten. Davon abgeleitet, finden sich am Ende einer jeden Phase gewisse Prüfpunkte in Form von einer Checkliste, die passend auf die jeweilige Beschaffung von Ihnen erweitert werden können beziehungsweise sollen.

Sollten Sie Fragen zu diesem oder andere Themen bezüglich Informationssicherheit haben, können Sie sich jederzeit gerne an das LSI wenden.

Phase 1: Analyse und Vorbereitung

Leitfragen:

- *Welche Anforderungen sollen mit der Beschaffung umgesetzt werden?*
- *Welche Aufgaben sollen einem Dienstleister übertragen werden und warum?*
- *Welcher Informationsverbund ist dabei betroffen?*
- *Welche Systeme sind diesem Informationsverbund zuzuordnen?*
- *Wird der komplette Informationsverbund ausgelagert? Falls nein, welche Schnittstellen werden benötigt?*
- *Müssen neben Vertraulichkeit, Integrität und Verfügbarkeit weitere wichtige Schutzziele hinsichtlich der auszulagernden Dienste / Prozesse beachtet werden?*
- *Existieren Gesetze oder Verordnungen, die zusätzlich beachtet werden müssen?*
- *Gibt es unternehmensinterne Vorgaben oder Richtlinien?*

In der Phase der Vorbereitung / Analyse werden alle wichtigen Informationen bezüglich der Beschaffung gesammelt und festgehalten. Diese Phase dient somit als unverzichtbare Voraussetzung für alle folgenden Phasen. Des Weiteren sollte zu diesem Zeitpunkt bereits abgewogen werden, ob es z.B. einer Auslagerung des Dienstes / Prozesses bedarf oder ob das Vorhaben auch intern gelöst werden kann. Der Auftraggeber muss sich im Klaren sein, welche Art von Produkt oder Dienstleistung er erwartet beziehungsweise benötigt und welche Systeme beziehungsweise Schnittstellen im entsprechenden Informationsverbund davon betroffen sind. Die für ihn wichtigen und einzuhaltenden Schutzziele haben dabei oberste Priorität und sind ein essentieller Bestandteil bei der Feststellung des jeweiligen Schutzbedarfs. Generell gilt, je höher der Schutzbedarf, desto höher sind auch die IT-Sicherheitsanforderungen. Zusätzlich kann eine Risikoanalyse dabei helfen Klarheit zu schaffen, ob sich aus informationssicherheitstechnischer Sicht Risiken herauskristallisieren, die mit entsprechenden technischen und/oder organisatorischen Gegenmaßnahmen behandelt werden müssen. Lässt sich beispielsweise ein Auslagerungsvorhaben nicht mit den Schutzzielen vereinen, so ist generell davon abzuraten. Bereits in dieser Phase sollte der Informationssicherheitsbeauftragte (ISB) und ggf. der Datenschutzbeauftrage (DSB) zu Rate gezogen werden.

Checkliste:

	Nr.	Prüfpunkt
Phase 1	1.1	Die Aufgaben, die das Produkt beziehungsweise der Dienstleister erbringen soll und der damit betroffene Informationsverbund, sind klar, eindeutig und vollständig beschrieben und schriftlich dokumentiert.
	1.2	Alle Schutzziele, die erreicht werden müssen, sind bekannt und dokumentiert.
	1.3	Weitere mögliche gesetzliche Regularien, die im Zusammenhang mit der zu erbringenden Dienstleistung stehen, wurden analysiert und werden beachtet.
	1.4	Auf Einhaltung von Unternehmensrichtlinien und -vorgaben wurde hinsichtlich der auszulagernden Geschäftsprozesse geachtet.
	1.5	Der ISB und ggf. der DSB wurden in den Beschaffungsprozess involviert.

Phase 2: Wahl geeigneter technischer und organisatorischer Vorkehrungen

Leitfragen:

- *Welche Service Level Agreements leiten sich aus diesen Schutzzielen ab?*
- *Welche Anforderungen an die Informationssicherheit müssen unter Berücksichtigung aller Aspekte aus Phase 1 umgesetzt werden?*
- *Welche Maßnahmen müssen sowohl auf seiten des Dienstleisters als auch auf Auftraggeberseite erfüllt werden?*
- *Was ist bei besonderen Situationen, wie z.B. bei Notfällen, zu beachten?*
- *Werden alle potentiellen Risiken durch geeignete Gegenmaßnahmen mitigiert (behandelt)?*

Noch vor der Auswahl eines Dienstleisters oder Produkts sollte dem Auftraggeber bekannt sein, welche nötigen technischen und organisatorischen Maßnahmen hinsichtlich des Beschaffungsvorhabens getroffen werden müssen. Dabei ist nicht nur die Seite des Dienstleisters zu betrachten, sondern auch die des Auftraggebers. Die erste Phase sollte demnach bereits alle Informationen bereitstellen, woraus sich ableiten lässt,

- welche technischen und organisatorischen Maßnahmen zu treffen sind
- und welche Service Level Agreements mit einem zukünftigen Dienstleister zu vereinbaren sind.

Des Weiteren ist es bereits zu diesem Zeitpunkt äußerst wichtig, gewisse Notfallszenarien zu durchdenken und dafür entsprechende Maßnahmen zu ermitteln. Beispiele dafür könnten das regelmäßige Backup, ständig erreichbare Ansprechpartner beziehungsweise funktionierende Kommunikationswege darstellen. Diese Maßnahmen sind auf dem ersten Blick vielleicht nicht unmittelbar ersichtlich, bei einem Notfall jedoch unabdingbar. Im Hinblick auf Produkte können Anforderungen an die IT-Sicherheit bestehen, die frühzeitig in das Leistungsverzeichnis aufgenommen werden müssen. Dies könnten beispielsweise Vorgaben des Auftraggebers sein, die nur einen bestimmten Nutzerkreis dazu berechtigen, auf gewisse Daten zugreifen zu dürfen. Diese Vorgaben kommen in der Regel von der Fachabteilung und sind noch nicht an den Sicherheitsvorgaben der IT-Abteilung oder des ISBs reflektiert.
Hilfe und Unterstützung bei der Wahl weiterer konkreter Maßnahmen bieten hierzu sowohl die Handlungsempfehlungen und Vorgehensmodelle des LSI für verschiedene kritische Infrastrukturen, als auch das Siegel 2.0 speziell für Kommunen.
Am Ende dieser Phase sollte dem Auftraggeber ein Lastenheft (Anforderungsliste) mit technischen und organisatorischen Maßnahmen hinsichtlich der Informationssicherheit in schriftlicher Form

vorliegen. Diese Liste dient unter anderem bei der Auswahl eines geeigneten Dienstleisters (Phase 3) sowie der späteren Planung und Vertragsgestaltung (Phase 4).

Checkliste:

	Nr.	Prüfpunkt
Phase 2	2.1	Alle technischen und organisatorischen Maßnahmen bezüglich Phase 1 wurden erkannt und in das Lastenheft (Anforderungsliste) aufgenommen.
	2.2	Bei einer Auslagerung von Geschäftsprozessen wurden generelle Maßnahmen wie • Zutritts-, Zugangs- und Zugriffskontrolle • Mandantentrennung (falls nötig) beachtet.
	2.3	Geltende Anschluss- beziehungsweise Teilnahmebedingungen wurden geprüft und werden beachtet.
	2.4	Notfallsituationen wurden durchdacht und weitere vorkehrende Maßnahmen daraus abgeleitet.
	2.5	Alle Risiken wurden am Ende klassifiziert und entsprechende Anforderungen zur Mitigation identifiziert.
	2.6	Ein Lastenheft (Anforderungsliste), in dem auch alle in 2.1 – 2.5 entwickelten Maßnahmen enthalten sind, wurde erstellt und liegt in schriftlicher Form vor.

Phase 3: Auswahl eines geeigneten Auftragnehmers

Leitfragen:
- *Worauf sollte bei der Wahl des Auftragnehmers geachtet werden?*
- *Wie kann sich der Auftraggeber von der Sorgfaltspflicht des Auftragnehmers überzeugen?*
- *Können (unangekündigte) Kontrollen durchgeführt werden?*
- *Wird der Dienstleister beziehungsweise das Produkt meinen Anforderungen im Lastenheft gerecht?*
- *Erbringt der Auftragnehmer alle Dienstleistungen selbst oder wird er Teile der Leistung extern vergeben (Subunternehmer)?*
- *Ist der Dienstleister zertifiziert (BSI-GS, ISO200x, ISIS12)?*

Eine geeignete Wahl hinsichtlich eines Auftragnehmers zu treffen ist nicht immer einfach und sollte vorher sorgfältig überlegt werden. Es spielen hierbei nicht nur die Kosten eine wichtige Rolle. So sollte der potentielle Auftragnehmer wirtschaftlich, finanziell und personell – jedenfalls für die gewünschte Vertragslaufzeit und jeweils in Bezug auf den Beschaffungsgegenstand – in der Lage sein, den Leistungsumfang des Auftrages und damit die Anforderungen an die IT-Sicherheit zuverlässig erbringen zu können. Im besten Fall ist der am Ende ausgewählte Auftragnehmer imstande, alle im Lastenheft beschriebenen Maßnahmen des Auftraggebers umzusetzen oder arbeitet bereits nach diesen Vorgaben.
Die nachfolgenden Punkte können bei der Wahl des Auftragnehmers für die Organisation hilfreich sein und bei der Entscheidung unterstützen:

Allgemein	Marktsondierung durchführen
	Erfüllung aller geforderten Anforderungen an die IT (Sicherheitskonzept, -ziele und -risiken beziehungsweise Anforderungsliste beachten)
	Bereitschaft des Auftragnehmers, die Standardverträge des Auftraggebers zu akzeptieren.
	Zertifikate, die Rückschlüsse auf das Sicherheitsniveau des Auftragnehmers geben (Achtung: der Geltungsbereich muss hierbei beachtet werden und sollte im Zusammenhang mit der zu erbringenden Beschaffung stehen!)
	Zeit der Markttätigkeit im ausgeschriebenen Bereich
	Allgemeiner Ruf / Reputation oder Erfahrungen anderer Kunden
	Öffentlich bekannte Sicherheitsvorfälle
	Bereits bekannte unter Vertrag stehende Unternehmen (Referenzunternehmen) / allgemeine Referenzen
	Standort der Verarbeitung (Sprachbarrieren, fremde Gesetzgebungen z.B. USA -> Patriot Act /CLOUD Act erlauben amerikanischen Regierungsbehörden Zugriffe auf die Daten, etc.)
	Vor-Ort-Besuch
+ Produktbezogen	Produktzertifizierungen
	Ausreichend Informationen und Dokumentation zur Zuverlässigkeit und zur Ausfallsicherheit der Produkte vorhanden
	EAL (Evaluation Assurance Level) Einstufung bei Hard- und Software beachten
	Verschlüsselung von Daten und des Transportwegs stehen zur Verfügung
	Verschlüsselungsmethoden entsprechen dem aktuellen Stand der Technik
	Benutzer- und Rechteverwaltung ist vorhanden
	Eine sichere Zwei-Faktor-Authentifizierung ist möglich
	Datensicherung und Wiederherstellung sind integriert
	Kompatibel zu bereits eingesetzten Software- und Hardwareprodukten
	Werkskonfiguration ist an den eigenen Bedürfnissen der IT-Sicherheit anpassbar (z. B. Systemhärtung, Deaktivierung von Datenweitergabefunktionen / „Heimfunken“ sowie abschalten nicht benötigter Dienste und Schnittstellen)
	Hardwaregeräte verfügen über ein redundantes Netzteil
	Sicherheitsanalyse (Penetrations- oder Schwachstellentests) werden durchgeführt

Checkliste:

	Nr.	Prüfpunkt
Phase 3	3.1	Alle Anforderungen aus dem Lastenheft können bezüglich der jeweiligen Beschaffung umgesetzt werden.
	3.2	Es wurde erfolgreich geprüft, ob der ausgewählte Auftragnehmer seinen Sorgfaltspflichten nachkommt und geeignet ist.

Phase 4: Vertragsgestaltung und weitere Vereinbarungen

Leitfragen:

- *Welche wichtigen Punkte gilt es im (Dienstleistungs-)Vertrag festzuhalten?*
- *Welche generellen Verpflichtungen und Rechte haben sowohl Auftragnehmer als auch Auftraggeber?*
- *Wie müssen die SLAs aussehen, damit den Anforderungen an die Sicherheit des Informationsverbunds entsprochen wird?*
- *Wie ist der Umgang mit Sicherheitsvorfällen definiert?*
- *Welche, auf das Produkt bezogene, Vertragsbestandteile müssen definiert werden?*
- *Ist der Dienstleister zertifiziert (BSI-GS, ISO2700x, CISIS12)?*
- *Ist eine Exit-Strategie möglich?*
- *Werden vom Dienstleister bei einem Rückbau der externen Dienstleistung alle Vorgaben erfüllt?*
- *Sind weitere Vereinbarungen anderweitig zu treffen?*

Nachdem die Wahl des zukünftigen Auftragnehmers hinsichtlich der Beschaffung getroffen wurde, müssen weitere relevante Prozesse geplant und schlussendlich vereinbart werden. Spätestens zu diesem Zeitpunkt sollten demnach folgende Punkte abschließend geklärt und geregelt sein:

- Werden zwischen Auftraggeber und Auftragnehmer regelmäßig Daten ausgetauscht (z.B. sicherer Filetransfer)?
- Bedarf es zwischen Auftraggeber und Auftragnehmer einer ständigen Netzanbindung für dauerhafte Zugriffe auf Systeme / Ressourcen (z.B. durch Site-to-Site VPN)?
- Wird Fernwartung durchgeführt werden?
- Werden beim Dienstleister Fremdpersonal, Subunternehmer etc. eingesetzt?
- Werden personenbezogene Daten verarbeitet?
- Existiert ausreichendes Know-how beim Auftraggeber oder besteht Schulungsbedarf?

Sollten diese Punkte relevant für die zu erbringende Beschaffung sein, ist es ratsam, entsprechende Regelungen vertraglich festzuhalten. Bei der Verarbeitung personenbezogener Daten ist zudem ein eigener Datenschutzvertrag in Bezug auf die Auftragsverarbeitung abzuschließen.

Die folgende Tabelle zeigt mögliche wichtige Bestandteile eines Vertrags auf, die es bei dessen Gestaltung zu berücksichtigen gilt (nicht abschließend):

Nr.	Vertragsinhalt
1	Beschreibung der Ziele und der Ausgangssituation (Abgrenzung).
2	Detaillierte Beschreibung des Leistungsinhalts und -umfangs.
3	Sicherheitskonzept und -ziele (Auflistung geeigneter technischer und organisatorischer Maßnahmen, die das Sicherheitsniveau des Auftraggebers mindestens erhalten beziehungsweise verbessern).
4	Kosten, z.B. Gesamtkosten oder Kosten je Vorgang, Kosten für den Abruf zusätzlicher, kurzfristig zu erbringender Leistungen, etc.
5	Verpflichtung des Auftragnehmers, dass permanent neueste Ausrüstung, Werkzeuge, Verfahren, Technologien, Updates/Patches zur Verfügung gestellt werden.
6	Verpflichtung zur regelmäßigen Aus- und Weiterbildung des Personals auf Seiten des Dienstleisters.
7	Servicezeiten (Service Level Agreement), z.B. 24/7 Ruf-Bereitschaft, etc.
8	Wartung (z.B. für Änderungsmanagement) • Fernwartung • vor Ort • zulässige Mittel, z.B. Ausgabe eigener Wartungslaptops • Wartungsfenster
9	Festlegung, ob und welche Arbeiten unter welchen Voraussetzungen an Subunternehmer vergeben werden dürfen.

10	Laufzeiten und Kündigungsrechte/-pflichten (Datenübergabe/Löschung).
11	Datenschutzvereinbarung (bei Auftragsverarbeitung).
12	Geheimhaltungsverpflichtung (Non Disclosure Agreement).
13	Schadenersatz und Vertragsstrafen bei Nicht- oder Schlechterfüllung der Dienstleistung.
14	Regelmäßig Berichterstellung und Termine, z.B. vierteljährlicher IT-Sicherheitsaustausch.
15	Notfallkonzept bei Ausfall (Business Continuity Plan BCP, Disaster Recovery Plan DRP) • Wiederanlaufzeiten • Max. Ausfallzeiten • Reaktionszeiten • Festlegung eines Eskalationspfades • ...
16	Kontrollrechte des Auftraggebers.
17	Standort der Dienstleistung.
18	Möglichkeit beauftragter Produkttests vor und während der Leistung.
19	Weitere Punkte, die aus Sicht des Auftraggebers und -nehmers wichtig sind.

Tabelle 1

Der CIO Bund bietet zudem auf seiner Webseite[1] „Aktuelle EVB-IT“ „Ergänzende Vertragsbedingungen zur Beschaffung von Informationstechnik“ Vorlagen an, die als Vorlagen für eine Beschaffung genutzt werden können.

Checkliste:

	Nr.	Prüfpunkt
Phase 4	4.1	Die Rechtsabteilung, der Informationssicherheitsbeauftragte, evtl. der Datenschutzbeauftragte und die Personalvertretung wurden eingebunden.
	4.2	Alle relevanten und wichtigen Punkte für Auftraggeber und Auftragnehmer wurden im Auslagerungs- beziehungsweise Dienstleistungsvertrag schriftlich festgehalten (siehe Tabelle 1).

Phase 5: Migration in den Betrieb

Leitfragen:

- *Gibt es Fallstricke bei der Übertragung der Aufgaben an den Dienstleister, die beachtet werden müssen?*
- *Muss die Aufnahme der Dienstleistung beziehungsweise die Einbindung eines neuen Produkts in die Infrastruktur störungsfrei bezüglich bestehender Prozesse beim Auftraggeber erfolgen?*
- *Sind die Schnittstellen zwischen internen und externen Services definiert, dokumentiert, aufgebaut und abgesichert?*

In der Migrationsphase wird die Übertragung der Aufgaben an den Dienstleister beziehungsweise die Einbindung des beschafften Produkts vorbereitet. Je nach Vorhaben wird dabei im Vorfeld untersucht, ob bereits laufende Prozesse beim Auftraggeber unterbrochen werden müssen oder die Dienstleistung vom Auftragnehmer einfach gestartet werden kann, da sie z.B. losgelöst ohne Auswirkung auf andere Prozesse ihren Platz findet. Am Ende dieser Phase geht die zu erbringende Dienstleistung beziehungsweise der Einsatz des neuen Produkts in den Produktivbetrieb über. Es

[1] www.cio.bund.de/Webs/CIO/DE/digitale-loesungen/it-beschaffung/evb-it-und-bvb/evb-it/evb-it-node.html, Stand 04.11.2022

empfiehlt sich, die ersten Wochen im Produktivbetrieb besonders auf Komplikationen oder andere Störhinweise zu achten, um schnellstmögliche Gegenmaßnahmen initiieren zu können („Migrationsbereitschaftsdienst“). Falls nötig kann eine Rollback-Strategie bei größeren Problemen helfen, den vorherigen Zustand aller Prozesse und somit den Produktionsbetrieb in angemessener Zeit wiederherzustellen.

Checkliste:

	Nr.	Prüfpunkt
Phase 5	5.1	Verantwortliche während der Migrationsphase wurden bestimmt und stehen bei Bedarf zu festgelegten Zeiten zur Verfügung.
	5.2	Kritische Geschäftsprozesse, die nicht unterbrochen werden dürfen, wurden ermittelt und entsprechende Konzepte für einen möglichen Ausfall bereitgestellt.
	5.3	Alle Anforderungen an die neue Dienstleistung beziehungsweise an das neue Produkt wurden analysiert und betroffene Prozesse angepasst beziehungsweise neue Prozesse etabliert.
	5.4	Eventuell benötigte maximale Ausfallzeiten wurden ermittelt, geplant und bekanntgegeben.
	5.5	Eine Rollback-Strategie wurde im Vorfeld entwickelt und kann bei Bedarf angewendet werden.

Phase 6: Laufender Betrieb

Leitfragen:

- *Werden Änderungen im Hinblick auf die vereinbarte Dienstleistung gemeinsam mit dem Auftraggeber besprochen?*
- *Sind „Kontrollen“ beziehungsweise ein Vergewissern der Einhaltung von vereinbarten technischen und organisatorischen Maßnahmen beim Dienstleister vorgesehen?*
- *Werden regelmäßige Kontrollen durchgeführt?*
- *Werden gemeinsame Notfallübungen durchgeführt?*
- *Sind Auditergebnisse des Dienstleisters für den Auftraggeber einsehbar?*

Nachdem die Migrationsphase erfolgreich beendet wurde, geht das Beschaffungsvorhaben in den “laufenden Betrieb“ über. Doch auch während einer laufenden Dienstleistung können sich Änderungen, wie z.B. das Einspielen von Updates oder ein Wechsel von Subunternehmern, seitens des Auftragnehmers ergeben. Hierbei ist es wichtig, bereits im Vorfeld das Vorgehen zusammen mit dem Auftragnehmer in den vorherigen Phasen abgestimmt zu haben, so dass seitens des Auftraggebers keine Geschäftsprozesse unerwartet und unwissentlich in Mitleidenschaft gezogen werden. Ein vereinbartes Vorgehen sollte auch im Hinblick auf Sicherheitsvorfälle definiert sein, um das Zusammenspiel zwischen Auftraggeber und Auftragnehmer für den Fall der Fälle zu regeln. Gemeinsame Notfallübungen können hierbei hilfreich sein und die Fähigkeiten der Mitarbeiter auf beiden Seiten im Umgang mit Sicherheitsvorfällen erhöhen.

Im besten Fall wurde an alle wichtigen Punkte für die Geschäftsbeziehung gedacht, diese geregelt und im Vertrag eindeutig festgehalten.

Checkliste:

	Nr.	Prüfpunkt
Phase 6	6.1	Der Auftraggeber besitzt die Möglichkeit, die Umsetzung der vereinbarten technischen und organisatorischen Maßnahmen beim Dienstleister hinreichend zu prüfen.
	6.2	Relevante Änderungen beim Dienstleister werden dem Auftraggeber gemeldet und ggf. mit ihm abgestimmt.
	6.3	Es existiert ein Konzept, wie bei potentiellen Sicherheitsvorfällen sowohl auf Seiten des Dienstleisters als auch auf Seiten des Auftraggebers vorzugehen ist.
	6.4	Es werden regelmäßig gemeinsame Notfallübungen durchgeführt.

Phase 7: Beendigung des Vertragsverhältnisses

Leitfragen:

- *Was muss der Auftraggeber und -nehmer bei Beendigung einer in Anspruch genommenen Dienstleistung beachten?*
- *Ist die Rückgabe von Betriebsmitteln geregelt?*
- *Ist die Rückübertragung von Daten an den AG geregelt?*
- *Werden nicht mehr benötigte Daten beim Dienstleister gelöscht?*
- *Werden alle Zutritte, Zugänge und Zugriffe, die nicht mehr benötigt werden, den entsprechenden Personen entzogen?*
- *Werden eigens für die Dienstleistung beziehungsweise für das Produkt vorgenommene Konfigurationen an Systemen (z.B. erstellte Firewall-Regeln) wieder zurückgesetzt / geändert?*
- *Müssen rechtliche Vorgaben eingehalten werden?*

Wie in der vorherigen Phase 6 erwähnt, ist es ebenso bei Beendigung eines Vertragsverhältnisses essentiell, entsprechende Punkte bereits im Vorfeld besprochen und im Vertrag eindeutig geregelt zu haben. Fehlende oder unzureichende Regelungen können sowohl für den Auftraggeber als auch für den Dienstleister zu einem problematischen Ende eines Vertragsverhältnisses führen. Folgende Punkte sind mögliche Beispiele (nicht abschließend), die bereits im Vorfeld zwischen den Vertragspartner geregelt sein sollten:

- Kündigungsfristen
- Rückgabe von Betriebsmitteln
- Umgang mit gespeicherten / gesammelten Daten (Aufbewahrungspflichten, Löschung, Aushändigung, ...)
- Entfernen von nicht mehr benötigten Berechtigungen / Freigaben etc.
- Spezielle rechtliche Vorgaben
- Vendor-Lock-In Problematik (d.h. durch bestimmte Gegebenheiten ist es nur noch schwer möglich, auf einen anderen Dienstleister zu wechseln)

Checkliste:

	Nr.	Prüfpunkt
Phase 7	7.1	Alle dem Dienstleister zur Verfügung gestellten Betriebsmittel wurden zurückgegeben.
	7.2	Entsprechende Berechtigungen (z.B. Zutrittsberechtigungen, Zugänge, Systemzugriffe, etc.) der involvierten Mitarbeiter wurden sowohl beim Dienstleister als auch beim Auftraggeber entzogen.
	7.3	Rechtliche Vorgaben, wie z.B. Aufbewahrungspflichten, werden eingehalten.
	7.4	Nicht mehr benötigte Daten, werden dem Auftraggeber zurückgegeben oder sicher gelöscht.

Quellen

[1] OPS.2.1: Outsourcing für Kunden, BSI (Stand Februar 2021)
[2] OPS.3.1: Outsourcing für Dienstleister, BSI (Stand Februar 2021)
[3] IT-Grundschutz-Methodik im Kontext von Outsourcing; BSI (Stand Dezember 2019)
[4] Sicheres IT-Outsourcing für Kommunen – Studie, Innovationsstiftung Bayerische Kommune (2. Auflage 2019)

Anhang

A1 Zusammenfassung aller Prüfpunkte

Nr.	Prüfpunkt
1.1	Die Aufgaben, die das Produkt beziehungsweise der Dienstleister erbringen soll und der damit betroffene Informationsverbund, sind klar, eindeutig und vollständig beschrieben und schriftlich dokumentiert.
1.2	Alle Schutzziele, die erreicht werden müssen, sind bekannt und dokumentiert.
1.3	Weitere mögliche gesetzliche Regularien, die im Zusammenhang mit der zu erbringenden Dienstleistung stehen, wurden analysiert und werden beachtet.
1.4	Auf Einhaltung von Unternehmensrichtlinien und -vorgaben wurde hinsichtlich der auszulagernden Geschäftsprozesse geachtet.
1.5	Der ISB und ggf. der DSB wurden in den Beschaffungsprozess involviert.
2.1	Alle technischen und organisatorischen Maßnahmen bezüglich Phase 1 wurden erkannt und in das Lastenheft (Anforderungsliste) aufgenommen.
2.2	Bei einer Auslagerung von Geschäftsprozessen wurden generelle Maßnahmen wie • Zutritts-, Zugangs- und Zugriffskontrolle • Mandantentrennung (falls nötig) beachtet.
2.3	Geltende Anschluss- beziehungsweise Teilnahmebedingungen wurden geprüft und werden beachtet.
2.4	Notfallsituationen wurden durchdacht und weitere vorkehrende Maßnahmen daraus abgeleitet.
2.5	Alle Risiken wurden am Ende klassifiziert und entsprechende Anforderungen zur Mitigation identifiziert.
2.6	Ein Lastenheft (Anforderungsliste), in dem auch alle in 2.1 – 2.5 entwickelten Maßnahmen enthalten sind, wurde erstellt und liegt in schriftlicher Form vor.
3.1	Alle Anforderungen aus dem Lastenheft können bezüglich der jeweiligen Beschaffung umgesetzt werden.
3.2	Es wurde erfolgreich geprüft, ob der ausgewählte Auftragnehmer seinen Sorgfaltspflichten nachkommt und geeignet ist.
4.1	Die Rechtsabteilung, der Informationssicherheitsbeauftragte, evtl. der Datenschutzbeauftragte und die Personalvertretung wurden eingebunden.
4.2	Alle relevanten und wichtigen Punkte für Auftraggeber und Auftragnehmer wurden im Auslagerungs- beziehungsweise Dienstleistungsvertrag schriftlich festgehalten (siehe Tabelle 1).
5.1	Verantwortliche während der Migrationsphase wurden bestimmt und stehen bei Bedarf zu festgelegten Zeiten zur Verfügung.
5.2	Kritische Geschäftsprozesse, die nicht unterbrochen werden dürfen, wurden ermittelt und entsprechende Konzepte für einen möglichen Ausfall bereitgestellt.
5.3	Alle Anforderungen an die neue Dienstleistung beziehungsweise an das neue Produkt wurden analysiert und betroffene Prozesse angepasst beziehungsweise neue Prozesse etabliert.
5.4	Eventuell benötigte maximale Ausfallzeiten wurden ermittelt, geplant und bekanntgegeben.
5.5	Eine Rollback-Strategie wurde im Vorfeld entwickelt und kann bei Bedarf angewendet werden.

6.1	Der Auftraggeber besitzt die Möglichkeit, die Umsetzung der vereinbarten technischen und organisatorischen Maßnahmen beim Dienstleister hinreichend zu prüfen.
6.2	Relevante Änderungen beim Dienstleister werden dem Auftraggeber gemeldet und ggf. mit ihm abgestimmt.
6.3	Es existiert ein Konzept, wie bei potentiellen Sicherheitsvorfällen sowohl auf Seiten des Dienstleisters als auch auf Seiten des Auftraggebers vorzugehen ist.
6.4	Es werden regelmäßig gemeinsame Notfallübungen durchgeführt.
7.1	Alle dem Dienstleister zur Verfügung gestellten Betriebsmittel wurden zurückgegeben.
7.2	Entsprechende Berechtigungen (z.B. Zutrittsberechtigungen, Zugänge, Systemzugriffe, etc.) der involvierten Mitarbeiter wurden sowohl beim Dienstleister als auch beim Auftraggeber entzogen.
7.3	Rechtliche Vorgaben, wie z.B. Aufbewahrungspflichten, werden eingehalten.
7.4	Nicht mehr benötigte Daten, werden dem Auftraggeber zurückgegeben oder sicher gelöscht.

Notizen: