Leitsätze 01 Finanzen / Haushalt / Bewirtschaftung

2021 Leitsatz 01/15 – Verantwortung der Bewirtschafter für ausgelagerte Bestandteile automatisierter Verfahren zur Bewirtschaftung von Haushaltsmitteln des Bundes

Leitsätze

(1) Bewirtschafter, die automatisierte Verfahren zur Bewirtschaftung von Bundesmitteln einsetzen, sind auch für die Ordnungsmäßigkeit ausgelagerter Verfahrensbestandteile verantwortlich.

(2) Die vollständige oder teilweise Auslagerung eines automatisierten Verfahrens an einen Dienstleister ist in einer Dienstleistungsvereinbarung zu regeln. Dabei sind auch die vom Dienstleister zu erbringenden Beiträge zum Internen Kontrollsystem für das Verfahren und der Abschluss einer Auftragsdatenvereinbarung nach der Datenschutzgrundverordnung zu berücksichtigen.

(3) Der Bewirtschafter muss nachhalten, ob der Dienstleister die vereinbarten Leistungen erbringt und somit einen ordnungsmäßigen Verfahrensbetrieb unterstützt. Hierzu sollte er sich beim Abschluss einer Dienstleistungsvereinbarung Prüfrechte beim Leistungserbringer sichern.

Hintergründe

(1) Jeder Bewirtschafter, der ein automatisiertes Verfahren zur Bewirtschaftung von Haushaltsmitteln des Bundes einsetzt, muss sicherstellen, dass das Verfahren ordnungsmäßig betrieben wird.[1] Dies gilt auch, wenn ein externer Dienstleister das automatisierte Verfahren betreibt oder einzelne Bearbeitungsschritte IT-gestützt durchführt, etwa das Einscannen von Unterlagen. Die Tatsache, dass sich das Verfahren oder Teile davon nicht mehr im direkten Delegationsbereich der/des Beauftragten für den Haushalt (BfdH) befindet, entbindet sie oder ihn nicht von der Verantwortung für die Ordnungsmäßigkeit des Verfahrens. Die

[1] Vgl. hierzu Nr. 1.1.1 Absatz 2 der Bestimmungen über die Mindestanforderungen für den Einsatz automatisierter Verfahren im Haushalts-, Kassen- und Rechnungswesen des Bundes (BestMaVB-HKR) i.V.m. Nummer 2 GoBIT-HKR.

Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik zu Verträgen mit Dienstleistern (z.B. beim Outsourcing von IT-Leistungen) sind grundsätzlich zu beachten.[2]

Der Bundesrechnungshof stellte bei seinen Prüfungen häufig fest, dass Bewirtschafter, die ihr automatisiertes Verfahren vollständig oder teilweise an Dritte auslagerten, sich der Gesamtverantwortung für das automatisierte Verfahren nicht bewusst waren. So lag etwa die Verfahrensdokumentation, die die Abläufe der eigenen und ausgelagerten Verfahrensbestandteile eindeutig und für einen sachverständigen Dritten verständlich beschreiben muss, bei den BfdH häufig nicht oder nur in Teilen vor. In den Gefährdungsanalysen, Sicherheitskonzepten und Notfallkonzepten blieben die ausgelagerten Verfahrensbestandteile oft unberücksichtigt, da die Bewirtschafter die von ihrem Dienstleister hierzu erhaltenen Informationen nicht mit ihren eigenen Dokumenten zusammenführten. Vielmehr gingen sie davon aus, dass der Dienstleister sich eigenverantwortlich um eventuell auftretende Probleme kümmern werde und sie selbst keinen Einfluss auf diese Abläufe nehmen müssten. Diese grundsätzliche Fehleinschätzung führte zu Verfahrensrisiken an der Schnittstelle zu den Dienstleistern, etwa durch weitgehend ungetestete, nicht vom Bewirtschafter freigegebene neue Verfahrensversionen.

Häufig hatten die Bewirtschafter auch die Benutzerverwaltung auf den Dienstleister ausgelagert. Sie kontrollierten in diesen Fällen meist nicht regelmäßig, ob die angelegten Benutzerkennungen und die vergebenen Rollen und Rechte im automatisierten Verfahren für die Aufgabenwahrnehmung noch erforderlich waren. Teilweise hatten sie auch keine Kenntnis über externe Benutzerkennungen, mit denen der Dienstleister auf das Buchführungssystem zugreifen konnte. Damit bestand das Risiko unberechtigter Zugriffe auf die Buchungsdaten.

(2) Wird ein automatisiertes Verfahren durch einen Dienstleister betrieben, sind die vom Dienstleister zu erbringenden Maßnahmen zur Gewährleistung eines ordnungsmäßigen Verfahrensbetriebes durch vertragliche Vereinbarungen sicherzustellen. Dienstleister, mit denen Dienstleistungsvereinbarungen geschlossen werden müssen, sind etwa zentrale Dienstleister des Bundes oder Dienstleister außerhalb der Bundesverwaltung. Aber auch mit der internen IT-Abteilung sollten Bewirtschafter entsprechende Vereinbarungen treffen, wenn diese das automatisierte Verfahren betreibt.

---

[2] Nr. 6.1.2 VV-ZBR BHO und Nr. 2 Absatz 1 Satz 1 BestMaVB-HKR.

In den Dienstleistungsvereinbarungen müssen die ausgelagerten Leistungen qualitativ und quantitativ genau beschrieben und Zuständigkeiten klar zugeordnet sein. Die auftragsspezifischen Details für die operative Umsetzung sind in Service- oder Pflegevereinbarungen zu den einzelnen Verfahren zu regeln. Hierin können neben vorgegebenen Wahlmöglichkeiten, wie Serviceklassen, Verfügbarkeitsregelungen, Entstörungszeiten, auch weitere kundenspezifische Anforderungen vereinbart werden.

Der Bundesrechnungshof stellte in seinen Prüfungen regelmäßig fest, dass Bewirtschafter keine Dienstleistungsvereinbarungen abgeschlossen oder die zu erbringenden Leistungen nicht vollständig und nachvollziehbar beschrieben hatten. So wurden beispielsweise Zuständigkeiten für eigene und ausgelagerte Verfahrensbestandteile, etwa für die Aufbewahrung von Belegdaten, nicht eindeutig geregelt. Dies galt insbesondere bei bereits langlaufenden Auslagerungsverträgen mit Dienstleistern, die inzwischen auf das ITZBund übergegangen sind. Hier waren die Vertragsbedingungen häufig nicht an zwischenzeitlich veränderte Anforderungen angepasst worden, so dass Auftraggeber und Auftragnehmer z. B. von unterschiedlichen Systemverfügbarkeiten und Servicezeiten ausgingen.

Auch forderten die Bewirtschafter die für ein funktionierendes Internes Kontrollsystem notwendigen Informationen beim Dienstleister oft nicht ein. So ließen sie sich z. B. keine regelmäßigen Auswertungen der Benutzerzugänge und -zugriffe vorlegen. Dies führte zu unkontrollierten Risiken in der Rechteverwaltung oder bei Datenschnittstellen zu den Dienstleistern, etwa weil Buchungsdaten von unberechtigten Personen einsehbar oder sogar manipulierbar waren.

Zu den Kontrollpflichten gehört auch der Abschluss einer Auftragsdatenvereinbarung nach Artikel 28 Satz 3 Datenschutzgrundverordnung (DSGVO). Sie ist erforderlich, damit die Bewirtschafter für die ausgelagerten Datenverarbeitungstätigkeiten ihrer datenschutzrechtlichen Verantwortung nach Artikel 24 Satz 1 DSGVO nachkommen können. Diese Vereinbarungen fehlten bisweilen oder waren nach mehreren Verfahrenserweiterungen nicht mehr aktuell.

(3) Der Bewirtschafter hat nach Nummer 1.1.1 Absatz 2 der Bestimmungen über die Mindestanforderungen für den Einsatz automatisierter Verfahren im Haushalts-, Kassen- und Rechnungswesen des Bundes (BestMaVB-HKR) dafür Sorge zu tragen, dass beim Einsatz des automatisierten Verfahrens die haushaltsrechtlichen Bestimmungen vollständig eingehalten

werden. Um dies sicherzustellen, muss er auch die ausgelagerten Verfahrensbestandteile regelmäßig prüfen. Hierzu sollte er beim Abschluss einer Dienstleistungsvereinbarung Prüfrechte beim Leistungserbringer vertraglich vereinbaren. Alternativ dazu könnte er vom IT-Dienstleister Prüfzertifikate Dritter (z. B. Bundesamt für Sicherheit in der Informationstechnik) verlangen, die die Einhaltung der haushaltsrechtlichen Vorgaben abdecken.

Der Bundesrechnungshof stellte häufig fest, dass Bewirtschafter ihre ausgelagerten Verfahrensbestandteile nicht oder nur eingeschränkt selbst prüften. Sie hatten meist auch keine entsprechenden Prüfrechte mit ihren Dienstleistern vertraglich vereinbart. Auch Prüfzertifikate Dritter über eingehaltene Standards und Richtlinien (z. B. DIN EN ISO/IEC 27001)[3] ließen sie sich in der Regel nicht vorlegen. Der Bundesrechnungshof stellte zudem fest, dass selbst standardmäßig durch den Dienstleister zur Verfügung gestellte Serviceberichte zu den ausgelagerten Verfahrensbestandteilen bei den Bewirtschaftern oft nicht vorlagen oder von diesen nicht ausgewertet wurden. Auch die Möglichkeit, zusätzliche Berichtspflichten zur Erhöhung der Verfahrenssicherheit zu vereinbaren, nutzten die Bewirtschafter in der Regel nicht. Damit kamen sie ihrer Gesamtverantwortung für den Verfahrenseinsatz oft nicht hinreichend nach.

[3] Die DIN EN ISO/IEC 27001 beinhaltet Anforderungen an ein Informationssicherheitsmanagementsystem, das mittelbar zur Informationssicherheit beiträgt. Diese internationale Norm kann von internen und externen Parteien dazu eingesetzt werden, die Fähigkeit einer Organisation zur Einhaltung ihrer eigenen Informationssicherheitsanforderungen zu beurteilen.