Prüfung des Projektes CURIAplus
Parlamentsdienste

Das Wesentliche in Kürze

Die Parlamentsdienste unterstützen die Bundesversammlung und ihre Organe bei der Erfüllung ihrer Aufgaben. Neben anderen Dienstleistungen stellen sie die Informatiksysteme und -anwendungen für die Bundesversammlung und die eigenen Mitarbeitenden bereit. Der Verwaltungsdelegation obliegt die oberste Leitung der Parlamentsdienste. Mit einer 2018 angenommenen Motion beauftragte das Parlament die Verwaltungsdelegation, die Digitalisierung des Rats- und Kommissionsbetriebs voranzutreiben und den Parlamentsdiensten die dafür notwendigen Aufträge zu erteilen. Die beiden IT-Projekte CURIAplus und Cervin sind dafür von zentraler Bedeutung.

Die Eidgenössische Finanzkontrolle (EFK) prüfte das strategische IT-Projekt CURIAplus. Weil dieses auf den Arbeiten des Projektes Cervin basiert, hat die EFK relevante Themen in diesem Vorhaben ebenfalls geprüft. Die EFK stellt fest, dass in beiden Projekten wesentliche Probleme und Risiken bestehen, insbesondere im Hinblick auf die Informationssicherheit. Die EFK kommt zum Schluss, dass die Ursachen mehrheitlich bei der ungenügenden Governance und Einhaltung von Weisungen sowie den fehlenden Architekturvorgaben zu finden sind. Aufgrund der Dringlichkeit hat die EFK am 30. April 2021 Vertreter der Geschäftsleitung der Parlamentsdienste und der Verwaltungsdelegation über die wesentlichen Erkenntnisse informiert. Die Parlamentsdienste haben die Feststellungen grundsätzlich als bereits bekannt eingestuft, diese aber anders beurteilt als die EFK.

Fehlende IKT-Strategie und IKT-Governance

Eine auf die Geschäftsziele oder auf den Digitalisierungsauftrag abgestimmte IKT-Strategie ist nicht vorhanden. Ebenso eine Betriebs- und Sourcing-Strategie und eine Ziel-Architektur, die alle relevanten Anforderungen berücksichtigen. In diesem Vakuum wurde von den Projekten – teilweise ohne umfassende Abklärung der Konsequenzen – Entscheide getroffen und Fakten geschaffen.

Im Mai 2021 haben die Parlamentsdienste das Engagement externer Spezialisten zur Erarbeitung der Grundlagen für eine IKT-Steuerung bekannt gegeben, was die EFK begrüsst. Bis zum Vorliegen der Arbeitsergebnisse bleibt offen, ob die von den Projekten eingeschlagene Richtung mit den übergeordneten Vorgaben kompatibel sein wird und ob Korrekturen bei Bedarf überhaupt möglich sind.

Die definitive Verabschiedung der seit 2018 erarbeiteten IKT-Governance wurde Anfang 2020 aufgeschoben. Dies unter anderem, weil Abhängigkeiten von der noch fehlenden IKT-Strategie erkannt wurden. Dieser Aufschub verstärkt unter Umständen bestehende interne Spannungen und Unsicherheiten betreffend Aufgaben, Verantwortlichkeiten, Kompetenzen sowie Prozessen bei IKT-Projekten und dem IKT-Betrieb.

Unklare Sicherheitsanforderungen und Nichteinhaltung von Weisungen und Richtlinien

Mit dem neuen Informationssicherheitsgesetz (ISG) werden der Verwaltungsdelegation Führungsaufgaben zur Informationssicherheit zugewiesen und eine übergeordnete Führung etabliert. Aufgrund der bisher geltenden Vorgaben, Weisungen und Richtlinien tragen die

einzelnen IKT-Projekte und die Parlamentsdienste die Verantwortung für angemessene Sicherheitsanforderungen und -massnahmen. Die EFK beurteilt diese Regelung angesichts der zunehmenden Digitalisierung und Bedrohungslage als nicht stufengerecht und begrüsst die vom ISG verlangte oberste Führungsverantwortung durch die Verwaltungsdelegation.

Die Projekte CURIAplus und Cervin halten geltende Richtlinien und Weisungen nicht ausreichend ein. Vorgeschriebene Sicherheitskonzepte bleiben im Anfangsstadium stecken. Arbeitsergebnisse wurden nicht wie vorgeschrieben erstellt und freigegeben. Somit sind nicht alle Sicherheitsanforderungen und -massnahmen in das Pflichtenheft, die Ausschreibung und den Werkvertrag aufgenommen worden.

Cervin: Undefinierter Betrieb, Support und fehlendes Outsourcingkonzept

Cervin (Parlnet) wird seit Ende 2019 von den Parlamentariern genutzt, wichtige Betriebsfragen bleiben aber weiterhin ungeklärt. Die Testmöglichkeiten sind ungenügend, es fand keine Abnahme statt und der Support wird von der Projektorganisation nach best effort wahrgenommen. Den Betrieb der Plattform haben die Parlamentsdienste ohne entsprechenden Vertrag und Service Level Agreement an eine externe Firma übertragen. Die von CURIAplus benötigten Deployment- und Test-Infrastrukturen sowie -Prozesse sind erst bruchstückhaft vorhanden. Ein projektübergreifendes Providermanagement und ein Betriebs- und Outsourcingkonzept fehlen.

Lücken in der Informationssicherheit bei Cervin mit Auswirkungen auf CURIAplus

Die Umsetzung von Sicherheitsanforderungen wurde in dieser Prüfung nicht systematisch geprüft. Das Sicherheitsniveau von Cervin ist gemäss extern durchgeführten Sicherheitsaudits unterdurchschnittlich. Es wurden Schwachstellen identifiziert, die gemäss Auditbericht schnellstmöglich behoben werden müssen, was nicht erfolgt ist. Aufgrund architektonischer bzw. technischer Grundsatzfragen ist unklar, ob die Behebung der Schwachstellen in allen Fällen möglich ist. Ausserdem fehlen Voraussetzungen, um zu erkennen, ob Angreifer bereits Sicherheitslücken ausgenutzt haben. Schwachstellen in Cervin wirken sich vielfach direkt oder indirekt auch auf CURIAplus aus, das mehr sensible Daten und Funktionen für die Parlamentarier zur Verfügung stellt.

Hohes Realisierungsrisiko für CURIAplus

Das von der Geschäftsleitung nach dem Projektabbruch von SOPRANO (einem weiteren Digitalisierungsprojekt) geforderte unabhängige Qualitäts- und Risikomanagement ist trotz fertiger Konzepte nicht etabliert. Eine unabhängige Beurteilung des Projektes bzw. der Projekt- und Risikoberichte fehlt. Im Risiko-Reporting des Projektleiters werden von internen Fachleuten gemeldete Risiken und solche aus externen Berichten nicht aufgenommen.

CURIAplus ist auf die rechtzeitige Fertigstellung von anderen IT-Projekten angewiesen, von denen einige bereits wesentliche Verzögerungen gemeldet haben. Die Entwicklung von CURIAplus ist nach einigen Monaten bereits im Rückstand und es bestehen Differenzen mit dem Lieferanten, ob das Projekt zum definierten Endtermin abgeschlossen werden kann. Dies führt bereits nach kurzer Zeit zu Diskussionen bezüglich Projektumfang und allfälligen Vertragsnachträgen.

Angesichts der Projektrisiken und der ungeklärten strategischen Vorgaben ist ausserdem zu klären, ob eine Sistierung des Projektes CURIAplus angebracht wäre. Nach Fertigstellung der übergeordneten Vorgaben müssen die laufenden Projekte jedenfalls an diese angepasst werden.