Parlamentarischer Vorstoss. Antwort des Regierungsrates

Vorstoss-Nr.: 297-2013
Vorstossart: Interpellation
Richtlinienmotion: ☐
Geschäftsnummer: 2013.1491

Eingereicht am: 14.11.2013

Fraktionsvorstoss: Nein
Kommissionsvorstoss: Nein
Eingereicht von: Sancar (Bern, Grüne) (Sprecher/in)

Weitere Unterschriften: 0

Dringlichkeit verlangt: Nein

RRB-Nr.: 600/2014 vom 7. Mai 2014
Direktion: Finanzdirektion
Klassifizierung: Nicht klassifiziert

Wo sind die hoch vertraulichen und sensiblen Daten des Kantons Bern gelagert?

Mit der Digitalisierung und der Anhäufung enormer Mengen gespeicherter Daten tauchen auch neue Probleme im Bereich des Datenschutzes auf. Viele Privatunternehmungen und Behörden lagern ihre hoch vertraulichen und sensiblen Daten zu Sozialhilfe, Justizverfahren, Steuern, KlientInnen- und Kundinnenprofile usw. in einer sogenannten Cloud -Struktur. Das heisst, die Daten und Programme werden auf Servern gespeichert, die in der Regel nicht in der Schweiz liegen, den Nutzenden über das Internet jedoch zu jeder Zeit zur Verfügung stehen. Die hoch sensiblen und vertraulichen Daten dürfen nur dann in einer Cloud abgelegt werden, wenn die Vertraulichkeit gewährleistet ist, das heisst, dass durch Verschlüsselung der Cloud-Anbieter nicht auf diese Daten zugegriffen werden kann. Je sensibler die Daten, desto umfangreicher müssen die organisatorischen, technischen und rechtlichen Anforderungen des Cloud-Service sein.

Der amerikanische Geheimdienst NSA zapft bekanntermassen im grossen Stile Datenströme an. Andere Geheimdienste tun dies bestimmt auch. Es stellt sich deshalb also die Frage, wo und mit welchen Sicherheitsmassnahmen die kantonalen Daten gelagert werden, wie die Vertraulichkeit gewährleistet ist und die Anforderungen des Berner Datenschutzniveaus erfüllt sind .

Der Regierungsrat wird daher gebeten, folgende Fragen zu beantworten:

1. Wo werden die hoch vertraulichen und sensiblen Daten des Kantons Bern gelagert?
2. Sind die Orte der Datenbearbeitung bekannt und werden Ortswechsel gemeldet und bewilligt?

3. Wer hat zu welchen Daten Zugang, wie ist der Zugang geregelt, um sicherzustellen, dass die sensiblen Daten nicht missbraucht werden können (4-Augenprinzip, Kontrollorgane etc.)

4. Entspricht das Datenschutzniveau bei einer Bearbeitung der Daten im Ausland den schweizerischen Anforderungen oder wurden zusätzliche Massnahmen vereinbart, wenn ja welche?

5. Ist das jeweils zur Anwendung gelangende Recht mit schweizerischem Recht vereinbar?

6. Wo befindet sich der Gerichtsstand? Was würde passieren, wenn der Gerichtsstand im Ausland ist und wie viel Kosten würde eine solche Auslagerung verursachen?

7. Wieviel kostet das vertrauliche Lagern der Daten, wie viel kostet eine Cloud-Lösung?

8. Wird der kantonale Datenschutzbeauftragte für den Cloud-Service beigezogen?

9. Wie schätzt der Regierungsrat das Risiko beim Cloud-Service ein und was gedenkt er falls nötig zu tun, um die Zulassung eines solchen für diesen Bereich der hoch sensiblen Daten zu verhindern?

Antwort des Regierungsrates

Zu Frage 1: Die Informatik und Telekommunikation (ICT) der Kantonsverwaltung ist zurzeit dezentral organisiert. Das Amt für Informatik und Organisation (KAIO) erbringt bestimmte Querschnittsleistungen, und die Direktionen und die Staatskanzlei (oder teils deren Ämter) sowie die Justiz und die kantonalen Anstalten und Unternehmen sind im Übrigen für ihre ICT-Grundversorgung und für den Betrieb ihrer Fachanwendungen – einschliesslich der Informationssicherheit – selbst verantwortlich. Daher kann eine Liste der Orte aller Datenbearbeitungen des Kantons ohne grossen Aufwand nicht erstellt werden. Dies gilt insbesondere für die Orte der Datenbearbeitungen durch ausgegliederte Träger kantonaler Aufgaben wie z.B. Spitäler, Heime oder Beratungsstellen. Die Publikation einer solchen Liste wäre auch aus Sicherheitsgründen problematisch. Zusammenfassend kann jedoch festgehalten werden, dass ein Grossteil der sensitiven Daten der Verwaltung, namentlich die Daten des Personal-, Finanz- und Steuerwesens sowie die harmonisierten Daten der Einwohner- und Stimmregister in den schweizerischen Rechenzentren der kantonseigenen Bedag Informatik AG bearbeitet und gespeichert werden. Eine Herausforderung ist die zunehmende Ausbreitung von mobilen ICT-Mitteln wie Smartphones und Tablets, die oft standardmässig mit ausländischen Cloud-Lösungen wie iCloud, OneDrive oder Google Drive verbunden sind. Es ist Aufgabe aller Behörden darauf zu achten, dass ihre Mitarbeitenden nicht schützenswerte staatliche Daten mit solchen Lösungen bearbeiten, weil diese den unten dargestellten rechtlichen Anforderungen oft nicht genügen.

Im Rahmen des laufenden Projekts zur unabhängigen Prüfung der Informatik in der Kantonsverwaltung (UPI) wird auch die Serverlandschaft der Verwaltung vertieft überprüft. Für Einzelheiten wird daher auch auf die den Aufsichtskommissionen des Grossen Rates vorliegenden Ergebnisse dieser Überprüfung verwiesen.

Zu Frage 2: Die Vorschriften der Kantonsverwaltung über Informationssicherheit und Datenschutz (ISDS) in der ICT finden sich in der Datenschutzgesetzgebung sowie in der Direktionsverordnung der Finanzdirektion vom 3. Januar 2011 über Informationssicherheit und Datenschutz (ISDS DV, BSG 152.040.2) und in den vom KAIO dazu erlassenen Ausführungsweisungen.

Die Allgemeinen Geschäftsbedingungen (AGB) der Kantonsverwaltung über ISDS, die laut den erwähnten Vorschriften in allen ICT-Verträgen eingesetzt werden müssen, verpflichten den Leistungserbringer zur Information über die Methoden und Prozesse, die er zur Erbringung seiner vertraglichen Leistungen einsetzt, so auch über den Ort der Leistungserfüllung. Der Auftraggeber kann die entsprechenden Unterlagen vor Ort einsehen und sich die betrieblichen Abläufe vorführen lassen. Zudem muss der Leistungserbringer den Auftraggeber unverzüglich über aussergewöhnliche Vorfälle informieren, die die Daten, Systeme und Prozesse des Auftrags betreffen, namentlich über ISDS-Verletzungen.

Der Ort der Datenbearbeitung ist auch ein Element der bei ICT-Projekten durchzuführenden ISDS-Analyse und des zu erstellenden ISDS-Konzepts. Eine Datenbearbeitung im Ausland ist nur zulässig, wenn ein angemessenes ISDS-Niveau gewährleistet ist (vgl. unten die Antwort auf die Fragen 4 und 5).

Zu Frage 3: Die vom KAIO erlassenen ISDS-Grundschutzregeln schreiben unter anderem vor, dass für alle Datenbearbeitungen Folgendes geregelt sein muss: Sicherheitszonen, Regelung der Zutrittsberechtigung, Schliessplan, Schliess- und Zutrittssystem, raumsichernde Massnahmen, Vergabe, Sperrung und Löschung von Benutzerkonten, Einsicht auf periphere Geräte, Authentifizierung, Protokollierung von und Sperrung wegen Fehlversuchen, Benutzerberechtigungskonzept, Weisungen für Datenübertragungsmittel, Benutzung von Netzwerkdiensten sowie Zugriffsbeschränkungen der Outsourcingpartner. Reichen diese Grundschutzmassnahmen nicht aus, muss ein ISDS-Konzept aufzeigen, mit welchen Massnahmen welche ISDS-Risiken reduziert werden. Die Antwort auf die gestellte Frage fällt daher je nach Anwendung unterschiedlich aus.

In der Kantonsverwaltung gibt es, anders als in der Bundesverwaltung, noch kein Verfahren zur Sicherheitsüberprüfung von Angestellten des Kantons oder Dritter, die sensitive Funktionen wahrnehmen. Dafür müssten gesetzliche Grundlagen geschaffen und personelle und finanzielle Mittel zur Verfügung gestellt werden. Auch eine Sicherheitsüberprüfung oder weiter ausgebaute Kontrollmechanismen können das Fehlverhalten Einzelner aber nie sicher verhindern.

Zu den Fragen 4 und 5: Die Bearbeitung von Daten im Ausland ist mit besonderen Risiken verbunden. Art. 14a des Datenschutzgesetzes[1] bestimmt daher im Einklang mit den bundesrechtlichen Vorschriften, dass Personendaten nicht ins Ausland bekannt gegeben werden dürfen – dazu gehört auch die Datenbearbeitung auf ausländischen ICT-Systemen – wenn eine Gesetzgebung fehlt, die einen angemessenen Schutz gewährleistet, es sei denn, dass hinreichende Garantien, insbesondere durch Vertrag, einen angemessenen Schutz im Ausland gewährleisten. Gemäss der Praxis der Bundesbehörden und den Wegleitungen des Eidg. Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) gilt das ausländische Datenschutzniveau als ausreichend, wenn Gesetzgebung und Praxis der Datenschutzkonvention des Europarates entsprechen. Der EDÖB führt eine Liste der Staaten, die diesen Anforderungen genügen; dazu gehören die Staa-

[1] Datenschutzgesetz vom 19. Februar 1986 (KDSG; BSG 152.04)

ten der EU. Gemäss der Wegleitung des EDÖB ist zudem die Datenbearbeitung in den USA zulässig, wenn die betreffende US-Unternehmung dem *U.S.-Switzerland Safe Harbor Framework* (http://export.gov/safeharbor) beigetreten und auf der entsprechenden Liste des *U.S. Department of Commerce* verzeichnet ist. In Bezug auf Staaten bzw. Anbieter, die diese Voraussetzungen nicht erfüllen, können stattdessen Vertragsklauseln gemäss den vom EDÖB veröffentlichten Musterbeispielen einen angemessenen Schutz vermitteln. Die für die Vergabe von ICT-Aufträgen verantwortlichen kantonalen Behörden müssen diese Rahmenbedingungen berücksichtigen und Massnahmen treffen, die die Einhaltung der ISDS-Vorschriften durch die Anbieter sicherstellen (Art. 3 Abs. 3 der Datenschutzverordnung[2]).

Die Vereinbarung besonderer schweizerischer Sicherheitsvorschriften ist aber gegenüber internationalen Grossunternehmen, die ihre Dienstleistungen stark standardisiert anbieten, oft nur schwer möglich. Zudem stammen die vorstehend genannten Vorschriften und Empfehlungen aus der Zeit vor dem Bekanntwerden des Umfangs der Informationsbeschaffung ausländischer Nachrichtendienste im Bereich von ICT-Systemen. Im Februar 2014 hat der Bundesrat bekanntgegeben, dass er basierend auf den Erkenntnissen zur aktuellen Bedrohungslage Betriebsleistungen für besonders kritische und zentrale Infrastrukturen der Bundesverwaltung wo möglich nur an Unternehmen vergeben will, welche ausschliesslich unter Schweizer Recht handeln, sich zur Mehrheit in Schweizer Eigentum befinden und ihre Leistung gesamtheitlich innerhalb der Schweizer Landesgrenzen erzeugen. Der Regierungsrat und die Kantonsverwaltung lassen sich auch von diesen Grundsätzen leiten.

Zu Frage 6: Gemäss den Allgemeinen Geschäftsbedingungen der Schweizerischen Informatikkonferenz (AGB SIK; www.sik.ch), die für alle ICT-Aufträge der Verwaltung Anwendung finden müssen, liegt der Gerichtsstand in der Schweiz. In Ausnahmefällen, etwa gegenüber Anbietern mit beherrschender Marktstellung, ist es nicht möglich, die Anwendung der AGB SIK zu vereinbaren. In diesem Fall müssen die verantwortlichen Behörden die Risiken eines ausländischen Gerichtsstands abwägen. Dieser bringt im Allgemeinen eine höhere Rechtsunsicherheit mit sich, und kann insbesondere in den USA im Streitfall zu viel höheren Prozesskosten führen.

Zu Frage 7: „Cloud“ (dt. „Wolke“) bezeichnet eine Form der massengeschäftlichen Erbringung von Informatikdienstleistungen über das Internet, bei der ein Anbieter nicht für jeden Kunden eine eigene Infrastruktur (z.B. eigene Server) aufbaut, sondern sich alle Kunden dieselbe Infrastruktur teilen, wobei ihre Daten allerdings logisch voneinander getrennt und nur von ihnen einsehbar sind. Diese Methode der Leistungserbringung hat Vorteile für die Kunden, da der Leistungsbezug oft verzugslos per „Selbstbedienung“ möglich ist, und für die Anbieter, die dank der möglichen massiven Skaleneffekte einen vorteilhafteren Preis anbieten können. Daher und wegen der zunehmenden internationalen Konkurrenz sind Cloud-Lösungen tendenziell günstiger als Lösungen mit dedizierter Infrastruktur, in einzelnen Bereichen sehr markant: Die Angebote grosser ausländischer Cloud-Anbieter wie Google, Amazon oder Microsoft können für Massenleistungen wie verwalteter Speicherplatz oder E-Mail um den Faktor hundert günstiger sein als die Angebote konventioneller Rechenzentrumsbetreiber. Allerdings gibt es viele verschiedene Cloud-Servicemodelle, die sich in Bezug auf Sicherheit und Kosten wesentlich voneinander unterscheiden können. Dazu gehören „infrastructure as a service“ (IaaS), bei der den Kunden nur Hardware-Infrastruktur angeboten wird; „platform as a service“ (PaaS), bei der virtuelle Server angeboten werden, auf denen die Kunden eigene Software laufen lassen können, oder „software /

[2] Datenschutzverordnung vom 22. Oktober 2008 (DSV; BSG 152.040.1)

business process as a service“ (SaaS / BPaaS), bei dem den Kunden spezifische Anwendungen oder ganze Geschäftsprozesse zur Verfügung gestellt werden. Allgemeine Aussagen zu den Sicherheits- und Kostenaspekten von Cloud-Lösungen sind daher nur mit Vorsicht möglich.

Zu Frage 8: Gemäss Art. 17a DSG muss die Datenschutzaufsichtsstelle für eine Vorabkontrolle beigezogen werden, wenn eine beabsichtigte Datenbearbeitung mit besonderen Datenschutzrisiken verbunden ist. Solche Risiken ergeben sich nicht bereits aus dem Cloud-Servicemodell an sich, aber Cloud-Lösungen sind häufiger mit erhöhten Risiken verbunden, insbesondere weil viele marktführende Cloud-Anbieter im Ausland tätig sind. In solchen Fällen wird die Datenschutzaufsichtsstelle zur Vorabkontrolle beigezogen und kann zur Lösung und zu den beabsichtigten Sicherheitsmassnahmen Stellung nehmen.

Zu Frage 9: Wie oben erwähnt stellt nicht in erster Linie das Cloud-Servicemodell an sich ein ISDS-Risiko dar. Riskant können vielmehr andere Aspekte sein, etwa der Ort der Datenbearbeitung, die bei allen ICT-Outsourcingaufträgen unabhängig vom Servicemodell zu beachten sind. Dazu wird auf die Antworten auf die vorstehenden Fragen verwiesen.

Jedoch ist bereits der heute unvermeidbare Einsatz von im Ausland entwickelter Hard- und Software mit dem Risiko verbunden, dass ausländische Nachrichtendienste gezielt Schwachstellen einbauen lassen und ausnutzen. Der Einsatz von Open-Source-Software, die in Bezug auf die Sicherheit transparenter ist, oder von Verschlüsselungstechnologien kann dieses Risiko bisher nur in einzelnen Bereichen reduzieren. Zudem kann der Verzicht auf die Nutzung der in Bezug auf ISDS potenziell riskanteren ausländischen Cloud-Massenlösungen auch den Verzicht auf die Realisierung von teils sehr wesentlichen Kostenreduktionen nach sich ziehen. Vor dem Hintergrund des Zielkonflikts zwischen der Reduktion von ISDS-Risiken und dem wirtschaftlichen Einsatz öffentlicher Mittel ist es aus der Sicht des Regierungsrates notwendig, die Entwicklung im Bereich der Informatiksicherheit aktiv zu verfolgen und im Einzelfall eine der jeweiligen Risikolage und den wirtschaftlichen Rahmenbedingungen angepasste Lösung zu finden. Das KAIO hat dazu ab 2014 im Rahmen einer Neupriorisierung der bestehenden Ressourcen seine Kapazität im Bereich der ISDS-Beratung ausgebaut.

An den Grossen Rat