BASEL LANDSCHAFT
REGIERUNGSRAT

Vorlage an den Landrat

Beantwortung der Interpellation 2022/479 von Laura Grazioli: «Breites Testen: Grundsätzliche Datenschutzfragen»
2022/479

vom 29. November 2022

1. Text der Interpellation

Am 1. September 2022 reichte Laura Grazioli die Interpellation 2022/479 «Breites Testen: Grundsätzliche Datenschutzfragen» ein. Sie hat folgenden Wortlaut:

> *Am 18. Januar 2022 wurden die Eltern der Schulkinder im Baselbiet darüber informiert, dass für das Breite Testen neue Prozesse etabliert worden seien, welche ab dem 24. Januar 2022 galten. Diese neuen Prozesse implizierten, dass fortan alle wesentlichen Identitätsmerkmale der Schulkinder (Personalien, ID-Nummer, Krankenkassennummer) registriert und den jeweiligen Speichelproben sprich dem entsprechenden DNA-Material zugeordnet wurden.*
>
> *Mit der Einführung dieses neuen Systems wurden diverse Datenschutzfragen aufgeworfen. Insbesondere stellte sich die Frage, wie der Datenschutz gewährleistet und wie verhindert wurde, dass keinerlei Missbrauchspotenzial im Zusammenhang mit den Daten und dem zugeordneten Genmaterial betrieben werden konnte. Diese Thematik wurde in der Fragestunde vom 10. Februar 2022 aufgenommen und teilweise beantwortet. Rückfragen beim Datenschutzbeauftragten des Kantons ergaben, dass die Situation in datenschutztechnischer Hinsicht gewisse zusätzliche Fragen aufwirft, deren grundsätzliche Klärung begrüssenswert wäre.*
>
> *Vor diesem Hintergrund wird der Regierungsrat gebeten, folgende Fragen zu beantworten:*
>
> *1. Sollen schützenswerte Daten wie Gesundheitsdaten generell im Ausland und konkret bei der Tochtergesellschaft eines US-amerikanischen Informatikdienstleisters gespeichert und bearbeitet werden dürfen?*
>
> *2. Wieso war es dem Kanton nicht möglich, z.B. gemeinsam mit anderen Kantonen oder mit dem Bund die Daten bei einem Schweizer Anbieter oder einer Verwaltungseinheit in der Schweiz speichern zu lassen?*
>
> *3. Welche Nacharbeiten stehen nun an, welche Lehren im Hinblick auf den Datenschutz zieht der Kanton aus diesem Fall und was sind die Optionen im Zusammenhang mit der weiteren Digitalisierung im Gesundheitswesen?*

4. Der Regierungsrat wies in der Fragestunde vom 10. Februar 2022 darauf hin, dass es «im Pandemiefall manchmal etwas schneller geht und man nicht dieselben Abklärungen machen kann wie man sie im Normalfall machen würde». Wie wird zukünftig die Risikoabwägung zwischen Datenschutz / Datensicherheit und Schnelligkeit in ausserordentlichen Situationen gemacht bzw. unter welchen Umständen ist die Regierung bereit, Kompromisse beim Datenschutz zu machen?

5. Vor dem Hintergrund der Informationen, die aus dem Breite Testen vorliegen einerseits, sowie der Diskussion zum Einsatz von Cloud-Services bei Verwaltungen in der ganzen Schweiz andererseits, stellt sich die Frage, ob der Kanton Baselland plant, zukünftig vermehrt Daten in der Cloud und / oder im Ausland zu speichern und bearbeiten? Falls ja:

a. Gibt es im Kanton konkrete Anweisungen, Richtlinien oder Vorgaben zum Einsatz von Cloud-Diensten oder der Bearbeitung von Daten im Ausland?

b. Was für Daten und mit welchen Rahmenbedingungen werden oder sollen zukünftig in einer Cloud und / oder im Ausland bearbeitet werden?

c. Gibt es Daten, die nach Einschätzung der Regierung nicht in einer Cloud und /oder im Ausland bearbeitet werden sollen?

d. Gibt es Bereiche, in welchen Clouds und / oder eine Bearbeitung im Ausland ein grosses Thema sind oder bereits intensiv genutzt werden?

e. Wie schätzt der Regierungsrat die Risiken beim Einsatz von Cloud-Diensten ein (beispielsweise bezüglich Vertraulichkeit, Datensouveränität, Kontrollverlust, Lieferantenabhängigkeit, Unübersichtlichkeit von Lieferketten (Subunternehmer) oder Zugriff durch ausländische Behörden)?

2. Einleitende Bemerkungen

Der Regierungsrat möchte vorab festhalten, dass der einleitende Abschnitt der Interpellation bereits Teil der *Frage 3 «Laura Grazioli: Breites Testen – Datenschutz / Fragestunde der Landratssitzung vom 10. Februar 2022 2022/24 vom 8. Februar 2022»* war. Dieser einleitende Abschnitt im Vorstoss kann aus folgenden Gründen falsch verstanden werden:

Die Aussage, dass *«wesentliche [..] Identitätsmerkmale der Schulkinder (Personalien, ID-Nummer, Krankenkassennummer) registriert und den jeweiligen Speichelproben sprich dem entsprechenden DNA-Material zugeordnet wurden»* geht von der Annahme aus, dass Informationen über die DNA von Schulkindern gespeichert und mit ihrer Identität in Verbindung gebracht würden. Dies trifft nicht zu.

Mit den PCR-Tests wird nicht die DNA von Personen bzw. Kindern analysiert bzw. sequenziert, sondern es wird eine Speichelprobe nach vorab genau definierten Teilen («Primer») der DNA des SARS-CoV2 (Corona-Virus) durchsucht.[1] Wird in einer Probe eine solche Sequenz gefunden, kann sie kopiert bzw. vervielfältigt werden, was zu einem positiven Testresultat führt. Wird in der Speichelprobe keine solche Sequenz des Virus gefunden, kann nichts kopiert werden; der Test fällt somit negativ aus. Nur der Befund (positiv oder negativ) wird gespeichert, das Probenmaterial wird anschliessend vernichtet. Somit kann auch nur der Befund anhand der Probennummer den Probanden zugewiesen werden. Das ist wichtig, damit diese über den Befund informiert und mit einem Testzertifikat bedient werden können. Es wird also keine DNA von Personen sequenziert

[1] Fact Sheet der National COVID-19 Science Task Force (NCS-TF) vom 29. Oktober 2020 mit Verweisen; abrufbar unter dem Link https://sciencetaskforce.ch/wp-content/uploads/2020/11/An_update_on_SARS-CoV-2_detection_tests29Oct20-EN.pdf (letztmals abgerufen am 20.10.2022).

und keine Information über DNA von Personen gespeichert. Die registrierte Information beinhaltet lediglich das Testergebnis betreffend eine allenfalls festgestellte Ansteckung mit SARS-CoV-2.

Die Verknüpfung des Testresultats mit den Personalien, der ID-Nummer der Speichelprobe und der Versichertennummer der Krankenkasse ist notwendig, um die betroffene Person über das Testresultat zu informieren, sie mit dem erforderlichen Zertifikat zu bedienen und um die Abrechnung der Testkosten durchzuführen. Der gesetzliche Auftrag zur Bekämpfung der Pandemie kann anders nicht erfüllt werden.

Sobald die erhobenen Daten für die Pandemiebekämpfung nicht mehr benötigt werden, ist mit diesen nach Artikel 88 der Epidemienverordnung (EpV; SR 818.101.1) in Verbindung mit Artikel 58 des Epidemiengesetzes (EpG; SR 818.101) zu verfahren. Die Archivierung anonymisierter Daten erfolgt nach dem kantonalen Informations- und Datenschutzgesetz (IDG; SGS 162).

Eine gesetzliche Grundlage, die hierfür notwendigen Speichelproben anders zu verwenden, als dies das EpG oder das Covid-19-Gesetz (SR 818.102) zur Bekämpfung der Corona-Pandemie vorsieht, besteht nicht.

Mit Blick auf die gesetzlichen Grundlagen und die aufgeworfenen Fragen betreffend die Sicherheit von Daten in Clouds bei US-Anbietern ist folgendes zu erwähnen:

Der noch in der Anfrage Grazioli (*Fragestunde der Landratssitzung vom 10. Februar 2022 2022/24 vom 8. Februar 2022*) erwähnte USA Patriot Act aus dem Jahr 2001 ist inzwischen im USA Freedom Act (2015) und hauptsächlich im USA Foreign Intelligence Surveillance Act (FISA) von 1978 aufgegangen.[2] Diese Gesetzesbestimmungen wurden in der Schweiz und der EU kritisiert, weil sie die Bestimmungen des Datenschutzes in der Schweiz und der EU unterlaufen.

Durch die Implementierung des «Privacy Shield EU-USA» bzw. des «Privacy Shield CH-USA» hätte ein Transfer von Daten in die USA auf EU- bzw. Schweizer Niveau weiterhin ermöglicht werden sollen. Der Europäische Gerichtshof (EuGH) hat mit der Entscheidung «Schrems II» (Urteil C-311/18 vom 26. Juli 2020[3]) das Abkommen «Privacy Shield EU-USA» für ungültig erklärt, womit auch feststand, dass das mehr oder weniger gleichlautende Abkommen «Privacy Shield CH-USA» die Mängel des US-Datenschutzes nicht beseitigen kann. Ein weiteres Problem für die Inanspruchnahme von amerikanischen Datenbearbeitern ist der Fakt, dass die amerikanischen Strafbehörden diese Unternehmen zur Herausgabe von Informationen zwingen können (CLOUD-Act). Dies auch dann, wenn die Datenbearbeitung nicht in den USA, sondern irgendwo sonst erfolgt. Der Kanton Basel-Landschaft geht aktuell davon aus, dass die Möglichkeit eines solchen Zugriffs in die Risikoanalyse einfliessen muss. Da die Rechtsprechung des EuGH für die Schweiz keine Rechtswirkung hat, behält sich der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) in seiner Beurteilung eine allenfalls anders lautende Entscheidung des Schweizerischen Bundesgerichts vor[4], vertritt jedoch nunmehr regelmässig die Auffassung, dass das «Privacy Shield CH-USA» kein adäquates Datenschutzniveau bietet.[5] Aufgrund dieser Entscheidung des EuGH haben die Europäische Kommission und die USA am 25. März 2022 eine neue Rahmenvereinbarung erreicht, mit welcher ein adäquates Datenschutzniveau zwischen der EU und der USA durch Anpassung von US-Amerikanischen

---

[2] Bureau of Justice Assistance, US Department of Justice - The Foreign Intelligence Surveillance Act of 1978 (FISA) – Justice Information Sharing (https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1286#14rkti; abgerufen am 21.10.2022)

[3] EuGH Rechtssache C-311/18 Data Protection Commissioner gegen Facebook Ireland Ltd und Maximillian Schrems (Vorabentscheidungsersuchen des High Court [Irland]) Urteil des Gerichtshofs (Große Kammer) vom 16. Juli 2020

[4] Stellungnahme [des EDÖB] zur Übermittlung von Personendaten in die USA und weitere Staaten ohne angemessenes Datenschutzniveau i.S.v. Art. 6 Abs. 1 DSG (PDF, 205 kB, 08.09.2020) (PDF, 205 kB, 08.09.2020) https://www.edoeb.admin.ch/dam/edoeb/de/dokumente/2020/Positionspapier_PS_%20ED%C3%96B_DE.pdf.download.pdf/Positionspapier_PS_%20ED%C3%96B_DE.pdf (abgerufen am 21.10.2022)

[5] Medienmitteilung des EDÖB vom 08.09.2020; abrufbar unter https://www.edoeb.admin.ch/edoeb/de/home/aktuell/medien/medienmitteilungen.msg-id-80318.html (abgerufen am 21.10.2022)

Gesetzen angestrebt werden soll.[6] Die US-Regierung hat am 7. Oktober 2022 eine *Executive Order* publiziert, mit der ein neues «EU-USA Privacy Framework» umgesetzt werden soll.[7] Der EDÖB ist zur Zeit daran, dieses auf die Tauglichkeit für ein «CH-USA Privacy Framework» zu überprüfen[8].

Für kantonale Aufgaben gilt das Informations- und Datenschutzgesetz. Für den Umgang mit Daten in Clouds, inkl. der Speicherung, hat die Konferenz der Schweizerischen Datenschutzbeauftragten das «Merkblatt Cloud-spezifische Risiken und Massnahmen» herausgegeben[9]. Die Aufsichtsstelle Datenschutz des Kantons hat zudem das «Merkblatt *Outsourcing durch öffentliche Organe*»[10] publiziert, das ebenfalls zu berücksichtigen ist. Für die Übermittlung von Daten ins Ausland kann zudem das Prüfschema des EDÖB (Anleitung für die Prüfung der Zulässigkeit von Datenübermittlungen mit Auslandbezug)[11] herangezogen werden. Der EDÖB rät von der Datenhaltung in Clouds von US-amerikanischen Unternehmen in Europa grundsätzlich ab, wenn die im Prüfschema erwähnten Garantien nicht gewährleistet werden können[12].

3. Beantwortung der Fragen

1. *Frage 1: Sollen schützenswerte Daten wie Gesundheitsdaten generell im Ausland und konkret bei der Tochtergesellschaft eines US-amerikanischen Informatikdienstleisters gespeichert und bearbeitet werden dürfen?*

Der Regierungsrat beabsichtigt keine generelle Bearbeitung und Speicherung von schützenswerten Daten im Ausland oder eine generelle Auftragsdatenbearbeitung bei US-amerikanischen Unternehmen (bzw. US-amerikanischem Recht unterliegenden Unternehmen). Er kann sich jedoch der Tatsache nicht entziehen, dass gerade auch US-amerikanische Informatikdienstleister schrittweise ihr Geschäftsmodell ändern: Das Marktangebot zur Nutzung von lizenzierbarer Technologie und Produkten in eigenen Rechenzentren wird zunehmend zu Gunsten von Dienstleistungsangeboten für Auftragsdatenbearbeitung (Cloud-Services) reduziert. Es kann aber auch beobachtet werden, dass die Anbieter aufgrund dringenden Anliegen der Auftraggeber gerade auch aus dem öffentlichen Bereich ihre Angebote anzupassen versuchen (bspw. Datenbearbeitung in EU oder CH) oder teilweise auch auf individuelle Voraussetzungen reagieren (Verhandlungen der SIK mit Microsoft zu Gerichtsstand und anwendbares Recht CH, Zweckbindung etc.). Dennoch sind dieser Marktentwicklung Privatpersonen, Unternehmen und Behörden weltweit ausgesetzt. Unter dieser Marktentwicklung und weiteren Aspekten der Organisation der Datenverarbeitung ist der Regierungsrat angehalten, alternative Produkte und Technologien oder eine fallweise Nutzung von Auftragsdatenbearbeitung unter Einhaltung der geltenden Informationssicherheits- und Datenschutzauflagen zu prüfen.

---

[6] European Commission – Questions & Answers: EU-U.S. Data Privacy Framework vom 07.10.2022; https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_6045 (abgerufen am 21.10.2022)
[7] The White House Briefing Room, FACT SHEET: President Biden Signs Executive Order to Implement the European Union-U.S. Data Privacy Framework (07.10.2022); https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/07/fact-sheet-president-biden-signs-executive-order-to-implement-the-european-union-u-s-data-privacy-framework/ (abgerufen am 21.10.2022).
[8] EDÖB Aktuell: European Union-U.S. Data Privacy Framework (EU-U.S. DPF) –- Der EDÖB hat das seitens der Vereinigten Staaten publizierte Factsheet betreffend das «Data Privacy Framework (DPF)» zur Kenntnis genommen und ist daran, dieses zu prüfen (07.10.2022); https://www.edoeb.admin.ch/edoeb/de/home/aktuell/aktuell_news.html#-1719342237 (abgerufen am 21.10.2022).
[9] Konferenz der Schweizerischen Datenschutzbeauftragten – Merkblatt Cloud-spezifische Risiken und Massnahmen; https://www.privatim.ch/wp-content/uploads/2022/02/privatim_Cloud-Merkblatt_v3_0_20220203_def._DE-1.pdf (abgerufen am 21.10.2022)
[10] Aufsichtsstelle Datenschutz BL – «Merkblatt "Outsourcing durch öffentliche Organe"» (Ausgabe 2014, in Überarbeitung); https://www.baselland.ch/politik-und-behorden/besondere-behorden/datenschutz/publikationen/merkblatter-musterschreiben/downloads-2/merkblatt-outsourcing-in-ueberarbeitung.pdf/@@download/file/Merkblatt%20Outsourcing%20in%20%C3%9Cberarbeitung.pdf (abgerufen am 21.10.2022)
[11] Anleitung [des EDÖB] für die Prüfung der Zulässigkeit von Datenübermittlungen mit Auslandbezug nach Art. 6 Abs. 2 lit. a DSG (veröffentlicht Juni 2021); https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/handel-und-wirtschaft/uebermittlung-ins-ausland.html#-2053327153 (abgerufen am 21.10.2022)
[12] vier «Garantien» gemäss Prüfschema der Anleitung für die Datenbearbeitung (FN 13): Klare Rechtsgrundlage, Notwendigkeit und Verhältnismässigkeit im Hinblick auf verfolgte Ziele, wirksame Rechtsbehelfe, Zugang zu einem unabhängigen und unparteiischen Gericht; andernfalls vollständige Verschlüsselung der Daten in der Cloud ('Bring your own key').

2. *Frage 2: Wieso war es dem Kanton nicht möglich, z.B. gemeinsam mit anderen Kantonen oder mit dem Bund die Daten bei einem Schweizer Anbieter oder einer Verwaltungseinheit in der Schweiz speichern zu lassen?*

Durch die Ergänzung vom 17. Dezember 2021 des Covid-19-Gesetzes mit dem Artikel 3 Absatz 6bis erhielten Personen, die sich im Rahmen von repetitiven Testungen in Betrieben, in Bildungseinrichtungen und in Gesundheitseinrichtungen mit gepoolten molekularbiologischen Analysen testen liessen, nunmehr bei einem negativen Testresultat ebenso Anspruch auf die Ausstellung eines Zertifikates (Art. 6a, Covid-19 Gesetz), wie dies bisher nur bei nicht gepoolten Tests der Fall war. Die dazu gehörende Verordnungsanpassung wurde bereits per 17. Januar 2022 in Kraft gesetzt. Sie war die Grundlage für den Einsatz einer «Zertifikatslösung» für das Breite Testen Baselland, welche in der vorgegebenen, kurzen Zeitspanne durch die gewählte, digitale Informationsbearbeitung umgesetzt werden konnte. Jede digitale Informationsbearbeitung ist von Restrisiken bezüglich Informationssicherheit und Datenschutz begleitet, dies gilt unabhängig vom Betriebsmodell der digitalen Lösung (verwaltungsintern oder Auftragsdatenbearbeitung). Generell sind diese Restrisiken bezüglich Informationssicherheit und Datenschutz mit den weiteren Risiken einer Verwaltungshandlung abzuwägen. Dies traf insbesondere während der «besondere Lage» im Zusammenhang mit der COVID-19-Pandemie zu, die im Dezember 2021 und Januar 2022 noch galt. In vorliegendem Fall galt es, die Risiken der gewählten digitalen Lösung gegen die eines mangelhaften Gesundheitsschutzes der Bevölkerung, einer mangelhaften Versorgungssicherheit oder einer mangelhaften Lagebeurteilungsmöglichkeit abzuwägen. Angesichts des Verlaufs der Pandemiebewältigung im Kanton Basel-Landschaft erachtet der Regierungsrat die durch den kantonalen Krisenstab erfolgten Abwägungen als zielführend und vertretbar.

3. *Frage 3: Welche Nacharbeiten stehen nun an, welche Lehren im Hinblick auf den Datenschutz zieht der Kanton aus diesem Fall und was sind die Optionen im Zusammenhang mit der weiteren Digitalisierung im Gesundheitswesen?*

Nach Einstellung des «Breiten Testen Baselland» (BTBL), werden die verbleibenden Daten, die nicht aufgrund der gesetzlichen Bestimmungen bereits zu löschen waren, ebenfalls gelöscht. Für das BTBL stehen im weiteren keine datenschutzrelevanten Nacharbeiten an.

Im Rückblick auf den Ablauf und das erreichte Ziel der «Sicherstellung der Gesundheit der Bevölkerung», vertritt der Regierungsrat die Auffassung, dass der Krisenstab, wie auch das zuständige kantonale Amt für Gesundheit, der Situation entsprechend korrekt gehandelt und entschieden haben. Der Aufbau und der Betrieb der notwendigen IT-Systeme erfolgte unter hohem zeitlichem Druck immer unter gebührender Beachtung des Datenschutzes und der Informationssicherheit. Dies vor dem Hintergrund des generellen Ansinnens des Regierungsrates, dass Fragen der Informationsflüsse, des Datenschutzes und der Informationssicherheit von Anfang an in die Planung von Lösungen einbezogen werden sollen.

Optionen zur weiteren Digitalisierung im Gesundheitswesen BL werden im Rahmen der laufenden Arbeiten im Amt für Gesundheit unter Berücksichtigung der Informationssicherheit und des Datenschutzes weiter analysiert und vorangetrieben.

4. *Frage 4: Der Regierungsrat wies in der Fragestunde vom 10. Februar 2022 darauf hin, dass es «im Pandemiefall manchmal etwas schneller geht und man nicht dieselben Abklärungen machen kann wie man sie im Normalfall machen würde». Wie wird zukünftig die Risikoabwägung zwischen Datenschutz / Datensicherheit und Schnelligkeit in ausserordentlichen Situationen gemacht bzw. unter welchen Umständen ist die Regierung bereit, Kompromisse beim Datenschutz zu machen?*

Wie der Regierungsrat bereits in der Fragestunde ausgeführt hat, sind Krisensituationen nicht mit dem Regelbetrieb vergleichbar. Entscheide müssen unter Zeitdruck und auf der Grundlage der zum Entscheidungszeitpunkt vorliegenden, meist unvollständigen, Informationen gefällt werden. Speziell im Bereich des Gesundheitswesens muss der Schutz von Leib und Leben oberste Priorität geniessen. Dabei werden datenschutzrechtliche und informationssicherheitsrelevante Themen, auch in der COVID-19-Pandemie, mitberücksichtigt; sie fliessen mittels Risiko-Abwägung in die Entscheide über das weitere Vorgehen mit ein.

Im Nachgang der Pandemie wurden bestimmte getroffenen Massnahmen und die zur Verfügung gestellten Lösungen für das breite Testen mit der Aufsichtsstelle Datenschutz (ASD) überprüft. Die festgestellten Punkte konnten bereinigt werden, und die Überprüfung ergab, dass die ASD weder einen Verstoss gegen geltende Bestimmungen des Datenschutzes festgestellt hat noch zur Ansicht gelangte, dass unter Berücksichtigung der ausserordentlichen Lage untragbare Risiken in Kauf genommen wurden.

5. *Frage 5: Vor dem Hintergrund der Informationen, die aus dem Breite Testen vorliegen einerseits, sowie der Diskussion zum Einsatz von Cloud-Services bei Verwaltungen in der ganzen Schweiz andererseits, stellt sich die Frage, ob der Kanton Baselland plant, zukünftig vermehrt Daten in der Cloud und / oder im Ausland zu speichern und bearbeiten?*

Obwohl sich allenfalls beispielsweise ein Anbieter einer Schweizer Steuerlösung mehr an den Anforderungen der nationalen Organe orientiert als ein Anbieter, der Lösungen für einen weiträumigeren Einsatz bereitstellt, sind die Behörden durch den zunehmenden Einsatz von Clouddiensten bzw. der Speicherung von Daten im Ausland vermehrt dazu gezwungen, abzuwägen, ob es überhaupt noch valable Alternativen gibt. Die Entwicklung auf dem Softwaremarkt zeigt, dass nicht nur international tätige Anbieter ihre Produkte vermehrt in der Cloud bereitstellen, sondern zunehmend auch kleinere, spezialisierte Hersteller. Das Angebot für die lokale «In House»-Installation oder den lokalen Betrieb nimmt laufend ab und wird, soweit es überhaupt noch verfügbar ist, wirtschaftlich immer unattraktiver, da Cloud-Dienste für Anbieter finanziell sehr interessant sein können.

Derzeit sind mehrere Projekte in Arbeit, die speziell die Speicherung von Daten in der Cloud und eine Auftragsdatenbearbeitung beabsichtigen, so beispielsweise das Projekt «Intranet-BL».

a. Gibt es im Kanton konkrete Anweisungen, Richtlinien oder Vorgaben zum Einsatz von Cloud-Diensten oder der Bearbeitung von Daten im Ausland?

Die Konferenz der Schweizerischen Datenschutzbeauftragten (privatim) hat das «Merkblatt Cloud-spezifische Risiken und Massnahmen» publiziert, auf das sich kantonale Behörden stützen können. Darauf aufbauend hat die Aufsichtsstelle Datenschutz BL eine Liste mit wichtigsten Anforderungen an eine Auftragsdatenbearbeitung erstellt, welche die privatim-Empfehlungen für die Verwaltung des Kantons Basel-Landschaft bezüglich zwingender Vorgaben und was mittels einer Risikoanalyse beurteilt werden kann, weiter konkretisiert.

Zusätzlich sind eine Vielzahl von verbindlichen Vorgaben für die IT in Kraft, die auch beim Einsatz von Clouddiensten zu berücksichtigen sind.

b. Was für Daten und mit welchen Rahmenbedingungen werden oder sollen zukünftig in einer Cloud und / oder im Ausland bearbeitet werden?

Es gibt derzeit keine Auflistung über bestimmte Datenbestände, die künftig in einer Cloud gespeichert werden sollen.

Projekte, in welchen Cloud-Lösungen in Betracht gezogen werden, sind sowohl aus der Sicht der Informationssicherheit als auch des Datenschutzes individuell zu beurteilen. Erst diese Beurteilung

und die Erfüllung der spezifischen Auflagen ermöglichen es, die bezeichneten Datenbestände in eine Cloudlösung auszulagern.

Wie in Antwort 5a ausgeführt, gibt es bereits Informatiklösungen für Datenbestände, die in der Cloud betrieben werden. So wurden z.B. die Prozesse für das Mitarbeitergespräch nach einer eingehenden Prüfung und Implementierung von relevanten Massnahmen in der Cloud umgesetzt. Als Gerichtsstand wurde die Schweiz vereinbart, als Ort der Bearbeitung der «EU-Access» (Stand Okt. 2020: DE und NL). Zudem wurde aufgrund der Risikobeurteilung entschieden, dass in der gewählten Lösung ausschliesslich «gewöhnliche» und keine besonderen Personendaten bearbeitet werden dürfen.

c. Gibt es Daten, die nach Einschätzung der Regierung nicht in einer Cloud und /oder im Ausland bearbeitet werden sollen?

Im konkreten Fall werden die Beurteilungsprozesse durchlaufen, die entweder eine Freigabe der Datenbestände für die Speicherung und allenfalls die Bearbeitung der Daten in der Cloud erlauben oder nicht. Grundsätzlich werden im Verlaufe der Zeit alle Verwaltungen Cloud-Services bereitstellen müssen, welche auch die Bearbeitung vertraulicher und streng vertraulicher Daten in der Cloud erlauben. Im Einzelfall wird zu prüfen sein, welche Cloudserviceanbieter die Voraussetzungen dazu erfüllen und wie die Services der kantonalen Verwaltung selbst dazu weiter zu entwickeln sind, um die Informationssicherheit und den Datenschutz mit vertretbaren Restrisiken gewährleisten zu können.

Die Speicherung von Daten im Ausland ist dabei differenziert zu betrachten. Es besteht grundsätzlich nicht die Absicht, Daten im Ausland zu speichern. Insbesondere sollen Nutzdaten, die nicht innerhalb der zentralen Verwaltung gespeichert werden können, in erster Linie in der Schweiz gespeichert verbleiben. Vorbehalten bleiben natürlich spezialgesetzliche Bestimmungen, die einer Bearbeitung im Ausland ohnehin entgegenstehen.

d. Gibt es Bereiche, in welchen Clouds und / oder eine Bearbeitung im Ausland ein grosses Thema sind oder bereits intensiv genutzt werden?

Derzeit sind bereits einige Bereiche produktiv im Einsatz, die auf einem Cloud-Ansatz basieren. Das bekannteste Beispiel für eine bestehende Cloud-Lösung ist der Internet-Auftritt des Kantons. Auch die Prozesse des «Mitarbeitendengesprächs (MAG) sind in einer Cloud-Lösung implementiert. Mit dem laufenden Projekt «Intranet BL» wird ebenfalls beabsichtigt, Daten in Microsoft Cloud-Services zu speichern.

Online verfügbar ist auch das Portal für Open Government Data (OGD). Hier werden nicht-vertrauliche Behördendaten ohne Schutzbedarf und frei von Rechten Dritter publiziert.

e. Wie schätzt der Regierungsrat die Risiken beim Einsatz von Cloud-Diensten ein (beispielsweise bezüglich Vertraulichkeit, Datensouveränität, Kontrollverlust, Lieferantenabhängigkeit, Unübersichtlichkeit von Lieferketten (Subunternehmer) oder Zugriff durch ausländische Behörden)?

Es gibt hierzu keine generelle Risiko-Einschätzung. Die Auslagerung von Daten und eine Auftragsdatenbearbeitung muss einzelfallweise geprüft werden, um dem jeweiligen Risiko gerecht zu werden. Grundlage ist die Einhaltung des Schweizer Datenschutzgesetzes bzw. die Datenschutz-Grundverordnung der Europäischen Union (DSGVO).

Abhängig vom Datenbestand, sind die Anforderungen im Einzelfall festzulegen. Sowohl bei einer Cloudlösung als auch bei einer intern betriebenen Lösung sind die Risiken mit geeigneten Massnahmen auf ein akzeptables Niveau zu reduzieren. Die Einhaltung der umzusetzenden Massnahmen ist anschliessend regelmässig zu überprüfen.

Aktuell ist für die geplante Nutzung von Microsoft Cloud Services für das Projekt Intranet BL eine entsprechende Risikoevaluation im Gang. Sie berücksichtigt nicht nur den Datenschutz, sondern auch die Aspekte der Informationssicherheit wie Datensouveränität, Kontrollverlust, Zugriff durch ausländische Behörden und Abhängigkeit von Lieferanten.

Liestal, 29. November 2022

Im Namen des Regierungsrats

Die Präsidentin:

Kathrin Schweizer

Die Landschreiberin:

Elisabeth Heer Dietrich