Kanton Bern
Canton de Berne

Datenschutzaufsichtsstelle (DSA)

Poststrasse 25
3072 Ostermundigen
+41 31 633 74 10
datenschutz@be.ch
www.be.ch/dsa

Ueli Buri
031 636 64 46
ueli.buri@be.ch

Datenschutzaufsichtsstelle, Poststrasse 25, 3072 Ostermundigen

Per «E-Mitwirkung»
Direktion für Inneres und Justiz
Münstergasse 2
Postfach
3000 Bern 8

Unsere Referenz: 2019.JGK.647
Ihre Referenz: 2019.JGK.647

14. August 2023

Totalrevision Datenschutzgesetz (KDSG) – Vernehmlassungsverfahren

Sehr geehrte Frau Regierungsrätin
Sehr geehrte Damen und Herren

Wir danken Ihnen für die Gelegenheit, im Rahmen der Vernehmlassung zum eingangs erwähnten Geschäft Stellung nehmen zu können.

Um unserem nachfolgenden Anliegen maximales Gewicht zu verschaffen, beschränken wir uns auf einen einzigen Punkt. Wir behalten uns jedoch vor, weitere (voraussichtlich untergeordnete) Anträge im Rahmen des 2. Mitberichtsverfahrens zu unterbreiten.

Antrag:

Auf die Variante 2 ist zu verzichten, Art. 15 Abs. 3 Bst. d ist ersatzlos zu streichen.

Begründung:

Vorgaben der Bundesverfassung (BV):

Art. 5 BV enthält Grundsätze rechtsstaatlichen Handelns, die so fundamental sind, dass auch der Gesetzgeber nicht davon abweichen kann. Dazu gehören das Legalitätsprinzip sowie die Wahrung des öffentlichen Interesses, der Verhältnismässigkeit und des Völkerrechts. Diese nicht verhandelbaren Grundsätze sind auch dann einzuhalten, wenn Grundrechte – hier auf informationelle Selbstbestimmung (Art. 13 BV) bzw. Datenschutz (Art. 18 KV) – eingeschränkt werden sollen (vgl. Art. 36 BV und 28 KV).

Die Datenschutzgesetze des Bundes (nDSG vom 25.09.2020, in Kraft ab 01.09.2023) und der Kantone konkretisieren das Verfassungsrecht. Jede Bearbeitung von Personendaten durch Behörden muss verfassungskonform sein, auch die Übermittlung an Auftragsbearbeiter im Ausland (BGE 144 I 126 E. 8.3.6 S. 152).

Art. 15 Abs. 1 des Vernehmlassungsentwurfs (VE-KDSG) verlangt deshalb zu Recht, dass das Grundrecht auf Datenschutz bei einer Bekanntgabe ins Ausland angemessen geschützt sein muss (vgl. auch Art. 16 Abs. 1 nDSG). Dies heisst nicht, dass der Empfängerstaat über ein identisches oder ähnliches *Datenschutzrecht* verfügen muss, sondern «nur», dass auch dort die nicht verhandelbaren *Grundsätze rechtsstaatlichen Handelns* garantiert sein müssen (so auch der Gerichtshof der Europäischen Union [EuGH] im Urteil C-311/18 vom 16.07.2020 [«Schrems II»], Rz. 94 und 105, sowie der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte [EDÖB] in seiner Anleitung für die Prüfung der Zulässigkeit

von Datenübermittlungen mit Auslandbezug, [Fassung vom Mai 2023], N. 05, mit Bezugnahme auf die Grundrechtsgarantien der Gesetzmässigkeit und der Verhältnismässigkeit sowie wirksamer Rechtsbehelfe durch Durchsetzung der Garantien vor einem unabhängigen Gericht).

Vorgaben des Völkerrechts:

Die gleiche Anforderung stellt das für die Schweiz und damit auch für den Kanton Bern (vgl. Art. 5 Abs. 4 BV) verbindliche Zusatzprotokoll zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten bezüglich Aufsichtsbehörden und grenzüberschreitende Datenübermittlung vom 08.11.2001 (SR 0.235.11).

Art. 2 Abs. 1 Zusatzprotokoll lautet:

1. Jede Vertragspartei stellt sicher, dass personenbezogene Daten nur dann an Empfänger, die der Rechtshoheit eines Staates, bzw. einer Organisation unterliegen, der bzw. die nicht Vertragspartei des Übereinkommens ist, übermittelt werden, wenn dieser Staat bzw. diese Organisation einen angemessenen Schutz für die beabsichtigte Datenübermittlung gewährleistet.

Nach N. 28 des Erläuternden Berichts zum Zusatzprotokoll kann die Feststellung eines angemessenen Datenschutzes für einen Staat generell (und nicht nur für eine einzelne Datenübermittlung in diesen) festgestellt werden. Davon macht Art. 15 Abs. 2 Bst. b VE-KDSG Gebrauch, wenn auf einen Feststellungsbeschluss des Bundesrates abgestellt wird.

Art. 2 Abs. 2 des Zusatzprotokolls lässt folgende Ausnahmen zu:

2. Abweichend von den Bestimmungen gemäss Absatz 1 des Artikels 2 dieses Protokolls kann jede Vertragspartei die Übermittlung personenbezogener Daten zulassen:

a. sofern dies im innerstaatlichen Recht vorgesehen ist:
   - um bestimmten Interessen des Betroffenen, bzw.
   - legitimen überwiegenden Interessen, insbesondere wichtigen öffentlichen Interessen, Rechnung zu tragen; oder

b. sofern Sicherheitsvorkehrungen, die sich insbesondere aus vertraglichen Klauseln ergeben können, von dem für die Übermittlung Verantwortlichen getroffen werden und diese nach Auffassung der zuständigen Behörde und in Übereinstimmung mit dem innerstaatlichen Recht angemessen sind.

Nach N. 31 des Erläuternden Berichts zum Zusatzprotokoll sind diese Ausnahmen restriktiv zu verstehen. So nennt der Bericht als wichtige öffentliche Interessen die in Art. 8 Abs. 2 EMRK erwähnten Fälle (d.h. nationale oder öffentliche Sicherheit, wirtschaftliches Wohl des Landes, Aufrechterhaltung der Ordnung, Verhütung von Straftaten, Schutz der Gesundheit oder der Moral, Schutz der Rechte und Freiheiten anderer).

Von den erlaubten Ausnahmen macht die Variante 1 von Art. 15 Abs. 2 und 3 VE-KDSG vollumfänglich Gebrauch:

- Art. 2 Abs. 2 Bst. a Zusatzprotokoll wird umgesetzt in Art. 15 Abs. 3 Bst. a–c VE-KDSG;
- Art. 2 Abs. 2 Bst. b Zusatzprotokoll wird umgesetzt in Art. 15 Abs. 2 Bst. c («andere hinreichende Garantien»).

Würdigung der Variante 2:

In der Variante 2 von Art. 15 Abs. 3 Bst. d VE-KDSG wird nun aber eine weitere Ausnahme für ausgelagerte Datenbearbeitungen vorgesehen, die selbst dann gelten soll, wenn keine hinreichenden Garantien vorliegen (!). Stattdessen soll es genügen, dass sich die verantwortliche Behörde vergewissert, dass der beauftragte Dritte eine dem Risiko angemessene Datensicherheit (vgl. Art. 10 Abs. 1 VE-KDSG) gewährleistet. «Sie gewichtet die öffentlichen Interessen der Behörden an der Nutzung der US-Cloud-Lösungen höher als die in dieser Variante als unwahrscheinlich betrachteten Eingriffe in die Grundrechte der betroffenen Personen».

Dabei argumentiert der Vortrag einerseits damit, dass die Behörden dank US-Cloud-Lösungen ihre Digitalisierungsziele viel rascher, kostengünstiger und kundenfreundlicher erreichen könnten, andererseits wird aber just **die eigene Strategie Digitale Verwaltung torpediert**, die das Vertrauen – insbesondere in Persönlichkeits- und Datenschutz sowie Datensicherheit – als elementare Voraussetzung für Bevölkerung und Wirtschaft zur Nutzung digitaler Dienstleistungen bezeichnet (Ziff. 2.4, S. 8).

Vor allem aber verkennt der Vortrag eine Reihe von Punkten, welche dazu führen, dass die **Variante 2 verfassungs- und völkerrechtswidrig** ist:

- Der Verzicht auf einen angemessenen Datenschutz bei Auftragsbearbeitungen ist nicht einfach ein (weiterer) Eingriff in das Grundrecht auf informationelle Selbstbestimmung, den der Gesetzgeber so vorsehen kann, sondern ein **unzulässiger Verzicht auf die Wahrung der nicht verhandelbaren Grundsätze rechtsstaatlichen Handelns nach Art. 5 BV**.

- Die Nutzung ausländischer Cloud-Lösungen durch kantonale Behörden – anstatt der «lästigen» Suche nach verfassungskonformen Alternativen – ist **kein anerkanntes wichtiges öffentliches Interesse im Sinne der Europaratskonvention und deren Zusatzprotokoll**. Vielmehr führt die Kapitulation vor der Marktmacht der internationalen Anbieter dazu, dass jene weiter steigt und die Anbieter keine Anstrengungen unternehmen müssen, um ihre Leistungen an die verfassungsrechtlichen Vorgaben der staatlichen Kunden anzupassen (ohne EuGH-Urteil in Sachen «Schrems II» hätte Microsoft nie ihre «EU Data Boundary» eingeführt).

  Die von den Regelungen des Bundes und der übrigen Kantone abweichende Variante 2 soll laut Vortrag einen «Standortvorteil» bringen. Dabei ist schwerlich erkennbar, für welchen Wettbewerb dieser Vorteil geschaffen werden soll: Die öffentlichen Verwaltungen stehen unseres Wissens in keiner Konkurrenz zueinander, und auch Bürgerinnen und Bürger sowie Unternehmen werden kaum vermehrt in den Kanton Bern umziehen, wenn ihre Daten in das unsichere Ausland übermittelt und dort bearbeitet werden. Wenn jemand einen Vorteil erfährt, dann höchstens die grossen Anbieter, die ihre Cloud-Lösungen im unkritischen Kanton Bern leichter verkaufen können als andernorts.

- Die unbelegte Annahme, dass bei einer Übermittlung von Personendaten in die USA Eingriffe in die Grundrechte unwahrscheinlich bzw. die Risiken für die betroffenen Personen nur theoretischer Natur und in der Praxis kaum relevant sind, ist eine **methodisch fragwürdige Behauptung** in doppelter Hinsicht: Die Risiken für die betroffenen Personen hängen ab von (a) der Eintrittswahrscheinlichkeit eines behördlichen Zugriffs auf die Daten und (b) den Folgen für die Person bei einem tatsächlich erfolgten Zugriff.

  (a) Für die Eintrittswahrscheinlichkeit ist es unstatthaft, von einem subjektiven Gefühl im Sinne von «es wird schon nicht passieren» auszugehen; vielmehr müsste anhand von relevanten, objektiven, zuverlässigen und überprüfbaren Quellen dargelegt werden, dass die Wahrscheinlichkeit eines Zugriffs *im konkreten Fall* so gering ist, dass sie als irrelevant betrachtet werden darf (nur dann erachtet der Europäische Datenschutzausschuss eine Datenübermittlung in ausländische Staaten mit einer problematischen Gesetzgebung als zulässig, vgl. Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten, Version 2.0 vom 18.06.2021, Rz. 43.3 – 47).

  (b) Eine Einschätzung der drohenden Nachteile bei einem tatsächlichen Behördenzugriff ist ohne Würdigung der *konkreten Inhalte der Daten* ebenfalls schlicht nicht möglich. Auch aus diesem Grund hat der Regierungsrat beschlossen, dass sensitive Personendaten nicht mit Cloud-Services von Microsoft bearbeitet werden dürfen. Es wäre deshalb völlig widersprüchlich, wenn der Gesetzgeber jetzt erlauben würde, dass Personendaten unabhängig von ihrer Sensitivität an jegliche ausländische Beauftragte übermittelt werden dürften.

  Die Annahme verkennt weiter, dass die **Verletzung** der verfassungsmässigen Garantien nicht erst dann eintritt, wenn eine ausländische Behörde tatsächlich auf vom Kanton Bern verantwortete Daten zugreift, sondern **schon bei deren Übermittlung in einen Rechtsraum, in dem die Grundsätze rechtsstaatlichen Handelns nicht mehr vollumfänglich gewährleistet sind**.

  Schliesslich würde die Variante 2 nicht bloss für Datenübermittlungen in die USA gelten, sondern in alle Länder ohne angemessenes Datenschutzniveau, also auch in solche mit teils gänzlich anderen Vorstellungen von Rechtsstaatlichkeit und Überwachung ihrer Bürgerinnen und Bürger. Mit diesem

weltweiten Schutzverzicht **schiesst die Variante 2 weit über die erklärte Absicht hinaus**. Sollte nämlich der Bundesrat dereinst (wie beim früheren «Privacy Shield») der EU folgen und mit den USA einen neuen Datenschutzrahmen CH-USA vereinbaren, so dass er die Angemessenheit des Datenschutzes bei Übermittlungen an teilnehmende Unternehmen feststellen kann, dann wird die Nutzung von US-Cloud-Lösungen wieder einfacher möglich sein, ohne dass dafür fundamentale verfassungsmässige Grundsätze missachtet werden müssen.

- Der **Vergleich mit dem privaten und privatwirtschaftlichen Umfeld ist verfehlt**: Nach Art. 5 Abs. 1 BV ist Grundlage und Schranke staatlichen Handelns das Recht. Dies bedeutet zweierlei: (1.) Der Staat darf nur handeln, soweit ihn das Gesetz dazu ermächtigt; dies gilt auch für die Bearbeitung von Personendaten (2.) Private dürfen alles tun, was ihnen der Staat nicht durch Gesetz verbietet; entsprechend dürfen sie Personendaten bearbeiten, soweit sie dabei die Persönlichkeit der betroffenen Personen nicht widerrechtlich verletzen (Art. 30 Abs. 1 nDSG). Urteilsfähige Menschen können für sich selbst entscheiden, ob sie einer Übermittlung ihrer Daten in «unsichere» Drittstaaten zustimmen wollen oder nicht. Und kommerzielle Datenbearbeiter haben selbst bei fehlender Zustimmung wenig zu befürchten, weil eine in ihren Rechten verletzte Person (i) dies überhaupt erfahren, (ii) gegen den Datenbearbeiter klagen sowie (iii) die Verletzung und einen Schaden beweisen müsste. Demgegenüber haben Behörden die Grundrechte von Amtes wegen zu beachten (Art. 35 BV und Art. 27 KV). Der Kanton Bern kann deshalb aus dem Verhalten der Privaten gar nichts für sich selbst ableiten.

Nebst den völker- und verfassungsrechtlichen Vorbehalten muss sich die Variante 2 **weitere Kritikpunkte** gefallen lassen:

- Entgegen der Beurteilung des Bundesrates, dass die USA gegenwärtig kein angemessenes Datenschutz aufweisen (Anhang 1 der Verordnung über den Datenschutz vom 31.08.2022), will der Kanton Bern US-Cloud-Lösungen gleich behandeln können wie in der Schweiz erbrachte IT-Dienstleistungen. Stellt der Bundesrat aber umgekehrt fest, dass ein Land ein angemessenes Datenschutzniveau aufweist, dann dürfen auch die bernischen Behörden dies als massgeblich erachten und müssen das Datenschutzniveau im Drittstaat nicht mehr selbst prüfen (Art. 15 Abs. 2 Bst. b VE-KDSG und zugehöriger Vortrag, S. 30 f.). Es entsteht der Eindruck, als möchte die Berner Verwaltung hier «**Rosinen picken**».
- Die Art. 44 ff. der Verordnung (EU) 2016/679 (DSGVO) verlangen für Datenübermittlungen aus der EU in Drittländer (wie die Schweiz) ein angemessenes Schutzniveau. Dazu steht im Vortrag: «Ein angemessenes Schutzniveau wird mittels Angemessenheitsbeschluss von der Europäischen Union bestätigt. Künftig erfolgt die Überprüfung der schweizerischen Gesetzgebung anhand der in der Datenschutz-Grundverordnung enthaltenen Anforderungen. Die Schweiz kann die Anforderungen erfüllen, indem sie das SEV Nr. 108+ umsetzt, da bei dessen Erarbeitung auf ein angemessenes Schutzniveau geachtet wurde» (Ziff. 2.1, S. 4). Wenn nun aber der Kanton Bern eine Regelung einführt, wonach bernische Behörden aus der EU übermittelte Personendaten ohne hinreichende Garantien an Auftragsbearbeiter in Länder ohne angemessenen Datenschutz übermitteln dürfen, dann kann dies den ausstehenden **Angemessenheitsbeschluss der EU-Kommission gefährden**.

Wir danken für die Berücksichtigung unseres Anliegens und stehen für Rückfragen zur Verfügung.

Freundliche Grüsse
Datenschutzaufsichtsstelle

Ueli Buri, Datenschutzbeauftragter