Kanton Bern
Canton de Berne

Datenschutzaufsichtsstelle (DSA)

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

Unsere Referenz: 2020.DSA.200 16. Juni 2023
Ihre Referenz: 2021.KAIO.530

Restrisiken beim Einsatz von M365 – Stellungnahme zum Bericht an den Regierungsrat

Sehr geehrter Herr Regierungspräsident
Sehr geehrte Mitglieder des Regierungsrates
Sehr geehrter Herr Staatsschreiber

Gerne nehmen wir zum Bericht «Restrisiken beim Einsatz von M365» des KAIO vom 7. Juni 2023 wie folgt Stellung.

A. Einleitende Bemerkungen

Zur rechtlichen Einordnung des Themas erlauben wir uns einleitend einige Hinweise: Die Bundes- und die Kantonsverfassung enthalten Garantien zugunsten der Rechtsunterworfenen – Bürgerinnen und Bürger sowie auch Mitarbeitende der Kantonsverwaltung – bei der Bearbeitung ihrer Personendaten durch die Behörden. Diese Garantien haben den Stellenwert von Grundrechten und umfassen namentlich das Erfordernis der Gesetzmässigkeit jeder Datenbearbeitung, die Beschränkung auf das zum erlaubten Zweck Notwendige (Verhältnismässigkeit) und den Schutz der Daten vor unbefugter Verwendung (Datensicherheit). Ihr Inhalt wird in der Datenschutzgesetzgebung weiter konkretisiert.

Es ist den Behörden grundsätzlich erlaubt, eine Bearbeitung von Personendaten an Dritte auszulagern (Auftragsbearbeitung). Dies darf jedoch nicht dazu führen, dass die Grundrechte der betroffenen Personen geschmälert werden. Für die Einhaltung der verfassungsmässigen Garantien bleiben die Behörden auch bei einer Auslagerung vollumfänglich verantwortlich. Sie müssen deshalb sicherstellen, dass sich die Auftragsbearbeiter ebenso an die Vorschriften zum Schutz der Grundrechte halten wie sie selbst es müssen. Dies erfordert eine entsprechende vertragliche Verpflichtung und geeignete Kontrollen, ob die vereinbarten Pflichten auch tatsächlich eingehalten werden.

Ist der Auftragsbearbeiter ein internationaler Anbieter von Online-Services mit einer weltweit verteilten Cloud-Infrastruktur (technische Einrichtungen und Supportorganisation), so ist – auch wenn der Vertrag Prüfrechte der Behörden und ihrer Aufsichtsbehörden vorsieht – **eine wirksame Kontrolle der Einhaltung der verfassungsmässigen Garantien nicht möglich**. Die hohe technische und organisatorische Komplexität der Leistungserbringung sowie sich laufend ändernde Umstände haben zur Folge, dass in wesentlichen Fragen **keine ausreichende Transparenz** besteht. Die nationalen Ansprechpersonen des Auftragsbearbeiters sind oft nicht in der Lage, verbindliche Angaben (z.B. über den genauen Ort einer Datenbearbeitung) zu machen, und wenn doch, dann handelt es sich meist um eine Momentaufnahme, welche schon morgen wieder überholt sein kann.

Der Einsatz von Cloud-Services – hier von Microsoft – führt deshalb naturgemäss zu zusätzlichen Risiken für die Grundrechte der betroffenen Personen. Damit diese Risiken als tragbar erscheinen können, hat sich der Regierungsrat zu vergewissern, dass die Services **unverzichtbare Vorteile gegenüber einer lokalen Lösung** bringen, welche die neuen Risiken aufzuwiegen vermögen.

B. Im Bericht beschriebene Risiken, Massnahmen und Restrisiken

Grundsätzlich dürfen wir feststellen, dass der Bericht die vom KAIO gemeinsam mit der DSA identifizierten Risiken vollständig und zutreffend beschreibt. Entsprechend können wir uns auf punktuelle Hinweise zu einzelnen Aussagen beschränken:

- **Zu Ziff. 2.2** (Stellenwert des Berichts): Der Bericht bezeichnet es als «wahrscheinlich, dass andere Berner Behörden, welche M365 einführen, zu einer anderen Einschätzung des Risikos gelangen und nicht dieselben Massnahmen umsetzen wie die hier vorgesehenen». Angesichts der allgemeinen Geltung der verfassungsmässigen Garantien einerseits und der generellen Natur der Cloud-spezifischen Risiken andererseits gehen wir nicht davon aus, dass andere Behörden zu einer gänzlich anderen Beurteilung der «Brutto-Risiken» (d.h. ohne Massnahmen) gelangen. Es hängt jedoch tatsächlich vom konkret beabsichtigten Einsatz von M365 ab, mit welchen Massnahmen die Risiken auf ein tragbares Mass gebracht werden können. Es ist deshalb richtig, dass die obersten Leitungsorgane von anderen Behörden in eigener Verantwortung über die Tragbarkeit der bei ihrem Einsatz von M365 verbleibenden Restrisiken werden entscheiden müssen.

- **Zu Ziff. 3.2** (Kontrollverlust gegenüber ausländischen Behörden): Eine verlässliche Beurteilung der Eintrittswahrscheinlichkeit von US-Behördenzugriffen auf in der Schweiz oder der EU gespeicherte Daten ist deshalb *nicht* möglich, weil vergangenheitsbasierte Prognosen mehrere Aspekte nicht berücksichtigen. (a) Den CLOUD Act gibt es erst seit 2018, der Beobachtungszeitraum ist deshalb zu kurz; (b) öffentliche Verwaltungen lagern erst jetzt allmählich Daten in Cloud-Dienste aus, weshalb Zugriffe auf Daten unter staatlicher Obhut überhaupt erst jetzt möglich bzw. interessant werden; (c) die US-Behörden können Microsoft verbieten, betroffene Kunden über den Zugriff zu informieren, weshalb weder die Vergangenheit vollständig bekannt ist noch die Prognose später validiert werden kann; (d) in interkontinentalen Verhältnissen kann sich die Zukunft völlig anders entwickeln als aufgrund der Vergangenheit erwartet (siehe die Frage einer möglichen Strommangellage). Zum betreffenden Risiko gehört deshalb, dass die Wahrscheinlichkeit seines Eintritts *unbekannt* bleibt.

  Die im Bericht erwähnten Massnahmen tragen diesem Umstand Rechnung. Es bleibt allerdings zu beachten, dass ein US-Behördenzugriff nicht nur auf Inhaltsdaten erfolgen kann, sondern auch auf Randdaten (insbes. Verkehrsdaten, d.h. wer wann mit wem kommunizierte), welche gegebenenfalls die Bildung von Profilen erlauben. Wir empfehlen deshalb als zusätzliche Massnahme, die Entwicklung der Behördenzugriffe – soweit bekannt – aktiv zu verfolgen und das Risiko bei Bedarf neu zu beurteilen.

- **Zu Ziff. 3.4** (Nichteinhalten von Bearbeitungsvorschriften): Wie getreu sich die Nutzenden an die Weisung «keine Daten mit erhöhtem Schutzbedarf in die Cloud» halten werden, wird wesentlich davon abhängen, wie einfach zugänglich und funktional die Alternativen sind, welche für die Bearbeitung von sensitiven Daten zur Verfügung stehen. Die Frage ist in den uns zur Vorabkontrolle unterbreiteten ISDS-Unterlagen bislang nicht adressiert worden, was uns zu einem Befund mit hoher Wesentlichkeit veranlasst hat.

C. Zusätzliche Hinweise

Schliesslich sind unseres Erachtens drei Hinweise anzubringen, welche in den beschriebenen Risiken nicht (ausreichend) zum Ausdruck kommen:

1. Vollständigkeit und Beherrschbarkeit von betrieblichen Risiken

Zur Aussage, dass der Bericht die Risiken vollständig beschreibt, ist ein Vorbehalt anzubringen. Das Modell der geteilten Verantwortung zwischen Microsoft als Erbringerin von hochstandardisierten Leistungen

und dem Kanton Bern als Leistungsbezüger macht das Erkennen, Bewerten und wirksame Bewältigen von betrieblichen Risiken zu einer sehr grossen Herausforderung, welche durch den raschen Technologiewandel und die Möglichkeit von Microsoft, tiefgreifende technische Veränderungen in rascher Folge und gegebenenfalls ohne aktive Steuerungsmöglichkeit des Kantons Bern einzuführen, weiter verstärkt wird. Wirksame Strategien der Kantonsverwaltung, die M365-Technoloie und deren rascher Wandel zu beherrschen, müssen zuerst erprobt werden und haben sich demzufolge (noch) nicht bewiesen.

Es besteht das Risiko, dass technologiebedingte Risiken von M365 für den Datenschutz und die Informationssicherheit nicht, unvollständig oder nicht rechtzeitig erkannt werden.

2. Umsetzung der Empfehlungen aus der Vorabkontrolle noch unklar

Im Rahmen der laufenden Vorabkontrollen der ISDS-Unterlagen zu einzelnen Komponenten des neuen M365-basierten kantonalen Arbeitsplatzes hat die DSA zahlreiche Feststellungen und Empfehlungen zu rechtlichen, organisatorischen, prozessualen und technischen Fragen formuliert und dem KAIO zur Stellungnahme unterbreitet. Weil die Frist dafür noch läuft, ist unklar, inwieweit die Empfehlungen der DSA umgesetzt werden (können). Zudem liegt ein wesentliches Dokument zur Beurteilung der Betriebssicherheit (noch) nicht vor, das gerade mit Blick auf den vorgenannten Punkt – das rechtzeitige Erkennen und Bewältigen von technologischen Risiken – von grosser Bedeutung ist.

Es besteht das Risiko, dass in der Vorabkontrolle festgestellte Mängel nicht behoben werden (können) und/oder keine vollständige Dokumentation zur Gewährleistung eines sicheren und datenschutzkonformen Betriebs vorliegt.

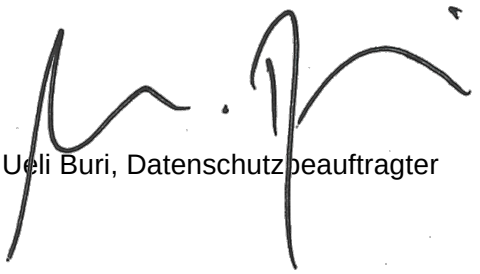
3. Verlust von digitaler Souveränität und ev. von Vertrauen der Betroffenen

Die vom Regierungsrat im Juni 2019 verabschiedete «Strategie Digitale Verwaltung des Kantons Bern» nennt als zentrale Anforderung an gute elektronische Behördendienstleistungen: «Vertrauen – insbesondere in Persönlichkeits- und Datenschutz sowie Datensicherheit – als elementare Voraussetzung für Bevölkerung und Wirtschaft zur Nutzung digitaler Dienstleistungen». Wie der Bericht des KAIO zeigt, führt der Einsatz von M365 zu verschiedenen Risiken, die auch dann, wenn der Regierungsrat sie als tragbar bewertet, nicht als unwesentlich bezeichnet werden können. Die grosse Abhängigkeit von einem amerikanischen Grosskonzern mit globaler Marktmacht gepaart mit der fehlenden Kontrolle über dessen Umgang mit den «Berner Daten» mögen sich zwar aktuell nur indirekt auf die digitalen Dienstleistungen der Kantonsverwaltung auswirken, können aber das Vertrauen der Bevölkerung und Wirtschaft in die digitale Souveränität bzw. Selbstbestimmung des Kantons Bern mindern.

Es besteht das Risiko, dass das Vertrauen von Bevölkerung und Wirtschaft in die Sicherstellung des Datenschutzes bei der Digitalisierung der Kantonsverwaltung geschmälert wird.

Freundliche Grüsse

Datenschutzaufsichtsstelle



Ueli Buri, Datenschutzbeauftragter