Kleine Anfrage

VwbP-Datendiebstahl

Frage von	Landtagsabgeordneter Achim Vogt
Antwort von	Regierungschefin Brigitte Haas

Frage vom 02. September 2026

In der Nacht auf den 30. Juli 2026 verschaffte sich eine unbekannte Täterschaft Zugriff auf das Verzeichnis wirtschaftlich berechtigter Personen (VwbP) und kopierte Daten von rund 31‘000 Rechtsträgern. Das Schweizer Bundesamt für Justiz hat die Einführung der E-ID zurückgestellt, weil künstliche Intelligenz den Online-Ausstellungsprozess unsicherer macht.

Die liechtensteinische Regierung setzt öffentlich auf die eID.li als Sicherheitsmassnahme. Eine digitale Identität schützt jedoch nicht vor einem unberechtigten Zugriff auf ein derartiges Register. Zudem hat die Regierung weitere Systeme mit sensiblen Daten vorsorglich vom Netz genommen.

* Wie ist es zu begründen, dass die Schweiz aufgrund von Sicherheitsbedenken die Einführung der E-ID zurückstellt und Liechtenstein als Antwort auf den Hackerangriff die eID zwingend für den VwbP-Einstieg vorschaltet?
* Für welche Systeme soll die neue Sicherheitsoptimierung durch die Vorschaltung der eID zukünftig gelten?
* Welchen Einfluss wird die angestrebte Sicherheitsoptimierung auf die E-Vertretung haben?
* Welche Erkenntnis gewinnt die Regierung in Bezug auf den Hackerangriff in Sachen Datensparsamkeit?
* Besteht die Möglichkeit, hochsensible Daten ausschliesslich auf einem eigenständigen, separaten Server in Liechtenstein zu speichern?

Antwort vom 04. September 2026

zu Frage 1:

Die Situation in der Schweiz betrifft den Ausstellungsprozess der staatlichen eID sowie damit verbundene Fragen des Datenschutzes, der digitalen Souveränität und der sicheren Identifikation von Personen im Registrierungsverfahren. Demgegenüber verfolgt die Nutzung der in Liechtenstein im Jahr 2020 eingeführten, gesetzlich verankerten eID.li beim Zugang zum Verzeichnis wirtschaftlich berechtigter Personen einen anderen Zweck, indem sie als vorgelagerte Authentisierungsmethode den Zugangsschutz zu digitalen Verwaltungsdiensten stärkt. Sie ermöglicht eine eindeutige elektronische Identifikation und ist Bestandteil eines mehrstufigen Sicherheitskonzepts.

zu Frage 2:

Die zusätzliche eID-Authentisierung kann grundsätzlich bei digitalen Diensten eingesetzt werden, bei denen durch eine zusätzliche Authentisierungsebene ein höheres Sicherheitsniveau erreicht wird. Die Beurteilung erfolgt risikobasiert und abhängig vom Schutzbedarf des jeweiligen Systems.

zu Frage 3:

Die Auswirkungen auf die eVertretung werden derzeit und periodisch analysiert. Allfällige zusätzliche Authentisierungs- oder Schutzmassnahmen werden risikobasiert geprüft und umgesetzt, sofern sie einen nachweisbaren Sicherheitsgewinn bringen und mit den fachlichen Anforderungen vereinbar sind. Bisher wurden keine konkreten Anpassungen bei der eVertretung vorgenommen und es sind derzeit keine geplant.

zu Frage 4:

Die bisherigen Erkenntnisse aus dem Vorfall bestätigen die Bedeutung der Grundsätze der Datensparsamkeit und Datenminimierung. Diese werden bereits heute berücksichtigt und sind bei der Weiterentwicklung bestehender sowie der Konzeption neuer Systeme weiterhin anzuwenden. Gleichzeitig sind die gesetzlichen Aufbewahrungs- und Dokumentationspflichten zu erfüllen.

zu Frage 5:

Die Möglichkeit, besonders schützenswerte Daten auf eigenständigen, separaten Systemen in Liechtenstein zu speichern, besteht. Sie wurde im vorliegenden Fall genutzt und ist somit bereits heute Teil der bestehenden Systemarchitektur.

Die Regierung prüft bei Systemen mit besonders schützenswerten Daten laufend, welche technischen und organisatorischen Massnahmen geeignet sind, um ein möglichst hohes Sicherheitsniveau sicherzustellen. Dazu kann auch der Einsatz technisch getrennter Infrastrukturen gehören. Die konkrete Ausgestaltung wird jeweils anhand des Schutzbedarfs, der gesetzlichen Anforderungen sowie der Verhältnismässigkeit beurteilt.