

Kleine Anfrage

Haftung und Verantwortung der eID.li

Frage von Landtagsabgeordneter Achim Vogt

Antwort von Regierungschefin Brigitte Haas

Frage vom 30. September 2026

Die staatliche digitale Identität eID.li ist seit Ende April 2020 verfügbar und ersetzt gemäss Art. 12 Abs. 1 E-GovG im behördlichen Verfahren die Unterschrift.»

Das eID.li-System wird von der Landesverwaltung geführt, die technische Umsetzung erfolgt über eine internationale private Auftragskette.

Am Anfang der Kette stehen die Hersteller der Endgeräte und die App-Stores von Apple und Google. Auftragsverarbeiterin ist die European Trust Services GmbH in Wien, ein Gemeinschaftsunternehmen der Österreichischen Staatsdruckerei GmbH und der CRYPTAS International GmbH. Unterauftragsverarbeiter sind die Younixx Identity AG in Wien, die Identity Trust Management AG (IDnow) in München und die Körbler GmbH in Wagna.

Im Juli 2025 hat die niederländische eMudhra B.V., Tochter der unter anderem im «Hi-Tech Defence and Aerospace Park» ansässigen indischen eMudhra Limited, die Mehrheit an CRYPTAS übernommen.

Keine dieser Firmen hat ihren Sitz in Liechtenstein. Der Staat verlässt sich auf diese Kette, ohne unmittelbaren Einfluss.

Deshalb stellt sich die Frage nach Haftung und Sanktionsmöglichkeiten.

- * Welche staatliche Stelle trägt gegenüber dem eID.li-Inhaber die rechtliche Gesamtverantwortung für Ausstellung, Betrieb und Sicherheit der eID.li?
- * Wer trägt die Beweislast, wenn ein eID.li-Inhaber bestreitet, eine mit seiner eID.li ausgelöste Handlung vorgenommen zu haben?
- * Wie hat die Regierung die 2025 erfolgte Mehrheitsübernahme von CRYPTAS International durch eMudhra - die auch Sicherheitslösungen für den Militärssektor und Satellitenkommunikation sowie KI-gesteuerte Systeme anbietet - hinsichtlich Sicherheit, Datenschutz und Haftung beurteilt?

- * Welche rechtlichen und technischen Schranken stellen sicher, dass die eID.li nicht zur Durchsetzung politischer oder ideologischer Vorgaben auf nationaler oder europäischer Ebene eingesetzt wird?
- * Welche Sanktions- und Durchsetzungsmöglichkeiten bestehen gegenüber den Firmen dieser Auftragskette, wenn Pflichten zu Sicherheit, Datenschutz oder Verfügbarkeit verletzt werden?

Antwort vom 02. Oktober 2026

zu Frage 1:

Die rechtliche Gesamtverantwortung für die eID.li trägt das Land Liechtenstein. Die Zuständigkeiten richten sich nach dem E-Government-Gesetz und der E-Government-Verordnung: Das Ausländer- und Passamt verantwortet das Ausstellungsverfahren, während das Amt für Informatik das eID-System betreibt, die Datensicherheit überwacht und die eingesetzten Lieferanten steuert. Externe Dienstleister erbringen technische Leistungen innerhalb der vom Land verantworteten Leistungserbringung. Ihre Beauftragung oder eine Änderung ihrer Eigentumsverhältnisse ändert nichts an den gesetzlichen Zuständigkeiten.

zu Frage 2:

Die Beweisregeln richten sich nach nationalem Recht. Nach Art. 6 des Personen- und Gesellschaftsrechts hat grundsätzlich jene Person die Tatsachen zu beweisen, aus denen sie einen Anspruch oder eine für sie günstige Rechtsfolge ableitet. Bestreitet ein eID.li-Inhaber eine mit seiner eID.li ausgelöste Handlung, besteht weder eine unwiderlegbare Zurechnung aufgrund der Verwendung der eID.li, noch eine allgemeine gesetzliche Beweislastumkehr zu seinen Gunsten. Macht er einen Haftungsanspruch geltend, hat er daher die anspruchsbegründenden Tatsachen nach den im Einzelfall geltenden materiell- und verfahrensrechtlichen Vorschriften nachzuweisen. Die Protokolldaten gemäss Art. 19 Abs. 4 des E-Government-Gesetzes können dabei als Beweismittel dienen und insbesondere Zeitpunkt und Kontext der eID-Nutzung nachvollziehbar machen. Die rechtliche Würdigung sämtlicher Beweismittel erfolgt im Einzelfall.

zu Frage 3:

Die Regierung hat die Mehrheitsübernahme von CRYPTAS International durch eMudhra zur Kenntnis genommen. CRYPTAS International ist nicht mit dem Betrieb des eID.li-Systems beauftragt. Unternehmen der CRYPTAS-Gruppe erbringen definierte technische Leistungen im Umfeld der für die elektronische Identifizierung eingesetzten Komponenten im Zusammenhang mit dem Identity Provider sowie die Bereitstellung von Zertifikaten.

Die Änderung der gesellschaftsrechtlichen Eigentumsverhältnisse bei CRYPTAS führte zu keiner Änderung dieser technischen Leistungen und zu keiner Änderung der gesetzlichen Zuständigkeiten für die eID.li. Für die Beurteilung der Sicherheit und des Datenschutzes sind insbesondere die konkrete Funktion eines Dienstleisters innerhalb der eingesetzten Infrastruktur, dessen tatsächlichen Zugriffsmöglichkeiten sowie die Einhaltung der gesetzlichen, vertraglichen und technischen Sicherheitsanforderungen massgebend.

zu Frage 4:

Die eID.li ist gesetzlich zweckgebunden. Nach dem E-Government-Gesetz dient das eID-System insbesondere der eindeutigen elektronischen Identifizierung, der Vertretung im elektronischen Geschäftsverkehr sowie der Freigabe beziehungsweise Übermittlung von Daten im Rahmen der gesetzlich vorgesehenen Anwendungsfälle.

Die Verarbeitung personenbezogener Daten erfolgt auf Grundlage der einschlägigen gesetzlichen Bestimmungen, insbesondere des E-Government-Gesetzes und der Datenschutzgesetzgebung. Sie unterliegt damit insbesondere den Grundsätzen der Rechtmässigkeit, Zweckbindung und Datenminimierung. Eine Verwendung der eID.li ausserhalb der gesetzlich vorgesehenen Zwecke bedarf einer entsprechenden Rechtsgrundlage.

Technisch und organisatorisch wird die Einhaltung dieser Vorgaben unter anderem durch Berechtigungskonzepte nach dem Need-to-Know-Prinzip, restriktive Administratorenrechte sowie die Protokollierung von Zugriffen und Änderungen unterstützt. Das E-Government-Gesetz schreibt ausdrücklich geeignete Massnahmen zur Gewährleistung der Datensicherheit sowie die Protokollierung der Zugriffe auf das eID-System vor.

Eine Verwendung der eID.li zur Durchsetzung politischer oder ideologischer Vorgaben ist rechtlich nicht möglich.

zu Frage 5:

Bei Sicherheitsverletzungen stehen dem Land je nach Rolle des Dienstleisters und Art der Pflichtverletzung vertragliche und gesetzliche Durchsetzungs- und Sanktionsmöglichkeiten offen. Dazu zählen datenschutzrechtliche Massnahmen sowie Schadenersatz- und Regressansprüche. Soweit vertraglich vereinbart, können auch Konventionalstrafen, Ersatzvornahmen, Sonderkündigungsrechte oder eine Vertragsbeendigung zur Anwendung kommen. Zusätzlich gelten die aufsichtsrechtlichen Vorgaben und die Schutz- und Haftungsbestimmungen der eIDAS-Verordnung.