25.082 BRG. Elektronisches Gesundheitsdossier. Bundesgesetz
Sitzung der SGK-N vom 20./21. August 2026

Kurzbericht vom 3. August 2026 zu den Auswirkungen einer «End-to-End»- Verschlüsselung beim E-GD

Auftrag an die Verwaltung - End-to-end Verschlüsselung

Die Verwaltung wird beauftragt, die konkreten Auswirkungen einer «end-to-end»- Verschlüsselung beim E-GD aufzuzeigen. Welche Konsequenzen sowie Vor- und Nachteile hätte eine solche Verschlüsselung, gerade auch im Hinblick auf das Opt-out-Modell?

Ausgangslage

Das elektronische Gesundheitsdossier (E-GD) soll zu einem zentralen Instrument für den digitalen Zugang zu Gesundheitsinformationen für die Bevölkerung in der Schweiz werden. Es ist eine Ablage für langfristig behandlungsrelevante Informationen und stellt diese den Inhaberinnen und Inhabern eines E-GD zur Verfügung. Insbesondere enthält das E-GD Informationen, die unabhängig von einzelnen Akteurinnen oder Institutionen verfügbar sein sollen, oder von denen man zum Zeitpunkt der Bereitstellung noch nicht weiss, wer sie als Nächstes benötigen wird.

Gleichzeitig soll das E-GD ein integraler Bestandteil des geplanten Gesundheitsdatenraums Schweiz (Swiss Health Data Space; SwissHDS) sein. In diesem Datenraum sollen dereinst Gesundheitsfachpersonen und Gesundheitseinrichtungen Daten strukturiert und standardisiert untereinander («business-to-business», B2B) austauschen können, beispielsweise Überweisungen, Aufträge oder Laborresultate. Während die B2B-Kommunikation im SwissHDS auf automatisierte Übertragung von Daten, auf maschinelle Effizienz und direkte Systemintegration ausgerichtet ist, dient das E-GD der Transparenz, der Souveränität seiner Inhaberinnen und Inhaber und der übergreifenden Versorgungskontinuität.

Angesichts der besonderen Sensibilität von Gesundheitsdaten hat sich der Bundesrat bei der Erarbeitung des Bundesgesetzes über das elektronische Gesundheitsdossier (EGDG) eingehend mit den sehr hohen Datenschutz- und Informationssicherheitsanforderungen auseinandergesetzt, deren Einhaltung für das E-GD unabdingbar sind. Ein hohes Schutzniveau ist massgeblich für das Vertrauen und die Akzeptanz sowohl der Bevölkerung als auch der Gesundheitsfachpersonen und ist damit für den Erfolg des E-GD von zentraler Bedeutung. Dieses Schutzniveau wird erreicht durch ein kohärentes Zusammenspiel technischer, organisatorischer und rechtlicher Massnahmen. Dazu zählen insbesondere robuste Authentifizierungsverfahren (Prozess der Identitätsprüfung), klare Zugriffsregelungen und eine revisionssichere Protokollierung der Zugriffe. Dieses geplante moderne und widerstandsfähige Sicherheitsarchitekturkonzept entspricht dem aktuellen Stand der Technik und wird kontinuierlich in Zusammenarbeit etwa mit dem Bundesamt für Cybersicherheit (BACS) sowie weiteren internen und externen Stellen weiterentwickelt, um das hohe Schutzniveau jederzeit sicherzustellen. Die Architektur wird nach den Prinzipien «Zero-Trust», «Security by Design» und «Security by Default» entwickelt und unterliegt den strengen Anforderungen des Bundesgesetzes über die Informationssicherheit (ISG; SR 128) und des Datenschutzgesetzes (DSG; SR 235.1). Die Daten des E-GD müssen nach Schweizer Recht und ausschliesslich in der Schweiz gespeichert werden. Analysiert wird auch, ob die Vertrauensinfrastruktur der elektronischen Identität (e-ID) sowie die Swiss Government Cloud genutzt werden können. Für das E-GD ist damit eine mehrstufige Sicherheitsarchitektur mit klaren Zugriffskontrollen vorgesehen; die durchgehende Verschlüsselung der Daten entspricht dabei dem heutigen Stand der Technik, ist bereits im geltenden elektronischen Patientendossier (EPD) umgesetzt und wird auch für das künftige E-GD beibehalten.

Gleichzeitig lassen sich Datenschutz- und Informationssicherheitsanforderungen nicht unabhängig von anderen Anforderungen regeln. Sie stehen in einem strukturellen Zielkonflikt mit anderen Dimensionen, der sich als Spannungsfeld zwischen Kosten, Sicherheit, Benutzerfreundlichkeit und digitaler Souveränität beschreiben lässt. So geht beispielsweise eine Erhöhung des Sicherheitsniveaus, etwa durch eine komplexere Verschlüsselung, zulasten der Benutzerfreundlichkeit und verursacht zusätzliche Kosten in Entwicklung und Betrieb. Diese Zielkonflikte müssen entsprechend sorgfältig ausbalanciert werden.

Darüber hinaus ist festzuhalten, dass das heutige EPD (wie auch das geplante E-GD) ein Sekundärsystem ist. Die Gesundheitsdaten bleiben auch in Zukunft dezentral dort gespeichert, wo sie initial aufgenommen werden – konkret in den Systemen bei Gesundheitsfachpersonen und Gesundheitseinrichtungen (Praxis- und Klinikinformationssysteme). Diese sind selbst für die sichere und datenschutzkonforme Datenhaltung verantwortlich. Die Datensicherheit eines Gesamtsystems bemisst sich letztlich am schwächsten Glied der Kette: Werden Daten an mehreren Orten gespeichert oder verarbeitet, vermag ein hohes Schutzniveau im E-GD eine schwächere Absicherung andernorts nicht zu kompensieren, da unrechtmässige Zugriffe und Datenabflüsse sich oft dorthin verlagern, wo der Widerstand am geringsten ist. Eine wirksame Sicherheitsarchitektur erfordert daher ein durchgängig gleichwertiges Schutzniveau über sämtliche Speicher- und Verarbeitungsorte hinweg, dessen Umsetzung jeweils in der Verantwortung der zuständigen Institutionen und Akteure liegt.

Ende-zu-Ende-Verschlüsselung (E2EE)

Verschlüsselt wird primär, um Informationen zu schützen beziehungsweise, um zu verhindern, dass Unbefugte auf sensible Inhalte zugreifen können. Dazu werden Daten mittels mathematischer Verfahren in eine unlesbare Form überführt. Sie können nur mit dem passenden Schlüssel wieder zurückgewandelt werden. Eine solche Verschlüsselung gespeicherter und übertragener Daten ist gang und gäbe und ein wesentlicher Pfeiler einer modernen Sicherheitsarchitektur: Sie ist das Fundament für Sicherheit, Souveränität und Vertrauen und damit weit mehr als eine technische Option. So findet praktisch jeder Abruf einer Webseite heute verschlüsselt statt. Im vorliegenden Kontext sind zwei unmittelbare Schutzziele der Informationssicherheit von besonderer Bedeutung: Erstens die Gewährleistung der Vertraulichkeit, indem Gesundheitsdaten ausschliesslich berechtigten Personen zugänglich sind. Zweitens die Begrenzung des Schadenspotenzials bei Cyberangriffen, indem unrechtmässig abgefangene oder entwendete Daten ohne die entsprechenden Schlüssel für Angreifer nutzlos bleiben.

Je nachdem, wer den Schlüssel besitzt, und an welcher Stelle die Verschlüsselung und Entschlüsselung erfolgt, lassen sich unterschiedliche Verschlüsselungsarten unterscheiden, welche jeweils ein unterschiedliches Schutzniveau und unterschiedliche Vertrauensvoraussetzungen mit sich bringen. Die Ende-zu-Ende-Verschlüsselung (End-to-end encryption, E2EE) stellt innerhalb dieses Spektrums eine von mehreren möglichen Ausprägungen dar. Sie selbst ist kein abschliessend definiertes und technisch einheitliches Konzept, sondern ein Sammelbegriff für eine Reihe unterschiedlicher Umsetzungsformen. Im Kern zeichnet sich sie sich dadurch aus, dass die kryptografischen Schlüssel ausschliesslich bei den Endpunkten – also bei den natürlichen Personen respektive den ihnen zuzurechnenden Geräten – liegen und verbleiben, Zwischenstationen (insbesondere die Infrastrukturbetreiberin) erhalten keinen Zugriff auf lesbare und verständliche Information.

Das Konzept selbst entfaltet seine Stärken vor allem in der gerichteten Kommunikation, wenn Absender und Empfänger im Voraus eindeutig bestimmt sind. Typische Anwendungsfelder sind daher Messenger-Dienste wie WhatsApp, die E-Mail-Verschlüsselung oder die sichere Übermittlung von Daten zwischen zwei definierten Systemen, so zum Beispiel auch bei der E-ID. Bei Konstellationen ohne im Voraus feststehenden Empfängerkreis ist E2EE konzeptionell nicht ohne Weiteres anwendbar. Ein anschauliches Beispiel hierfür liefern Gruppenchats: Neu hinzukommende Mitglieder können technisch bedingt nicht auf früher versendete Nachrichten zugreifen, da diese ausschliesslich für die zu diesem Zeitpunkt bekannten Empfängerinnen und Empfänger verschlüsselt wurden.

E2EE kann in bestimmten Situationen den Vorteil bieten, dass ein höheres Schutz- bzw. Vertrauensniveau insbesondere gegen Insider-Zugriffe und interne Datenlecks bei der Betreiberin erreicht

werden kann. Demgegenüber steht als Nachteil, dass infrastrukturseitige Funktionen wie Prüfung auf Schadsoftware, Volltextsuche oder automatisierte Auswertungen erheblich erschwert oder gar verunmöglicht werden, da die Daten für das System selbst nicht lesbar sind. Verschlüsselung im Sinne von E2EE kann bestehende Prozesse verkomplizieren und aufwändiger machen, denn diese Verschlüsselungsmethode erfordert ein anspruchsvolleres Schlüsselmanagement auf den Endgeräten. Das erhöht die Komplexität bei Implementierung, Wiederherstellung und Multi-Geräte-Nutzung gegenüber anderen Methoden deutlich. Damit verbunden sind regelmässig höhere Kosten. Geht ein Schlüssel verloren (z.B. ein Smartphone mit dem gespeicherten Schlüssel), sind alle damit verschlüsselten Daten unzugänglich, sofern kein Verfahren zur Schlüsselwiederherstellung existiert. Ein solches Wiederherstellungsverfahren würde jedoch dem Grundsatz einer strikten E2EE-Verschlüsselung widersprechen, da es zwangsläufig eine Instanz voraussetzt, die auf den Schlüssel oder eine Kopie davon zugreifen kann. Bei der Langzeitspeicherung kann der Verlust eines Schlüssels ohne entsprechendes Verfahren den dauerhaften Verlust aller je abgelegten Daten bedeuten – ein für viele Anwendungsfälle inakzeptables Risiko.

Im internationalen Vergleich zeigt sich denn auch: Es ist kein staatliches oder landesweites EPD-System bekannt, das eine strikte E2EE-Verschlüsselung für Informationen nutzt, auf welche von unterschiedlichen Behandlungsseiten zugegriffen wird.

Die grosse Herausforderung beim E-GD ist, dass Daten nicht einfach übermittelt, sondern längerfristig gespeichert werden - oft ist zudem nicht im Voraus klar, wer später auf die Daten zugreifen soll. Das unterscheidet sich deutlich von Anwendungen wie WhatsApp oder E-Mail. Zudem stellt E2EE Kernfunktionen wie den Notfallzugriff oder die automatische Eröffnung von E-GD in Frage, denn alle Inhaberinnen und Inhaber müssten dabei einen kryptografischen Schlüssel für ihr E-GD generieren. Schliesslich stellt E2EE im Kontext des E-GD deutlich höhere Anforderungen an die Digitalkompetenzen der Inhaberinnen und Inhaber (Stichwort digitale Inklusion und Barrierefreiheit) als auch der Gesundheitsfachpersonen, die bereits sonst mit zunehmenden administrativen Aufgaben stark belastet sind.

Ergebnisse externe Analyse der ETH Lausanne

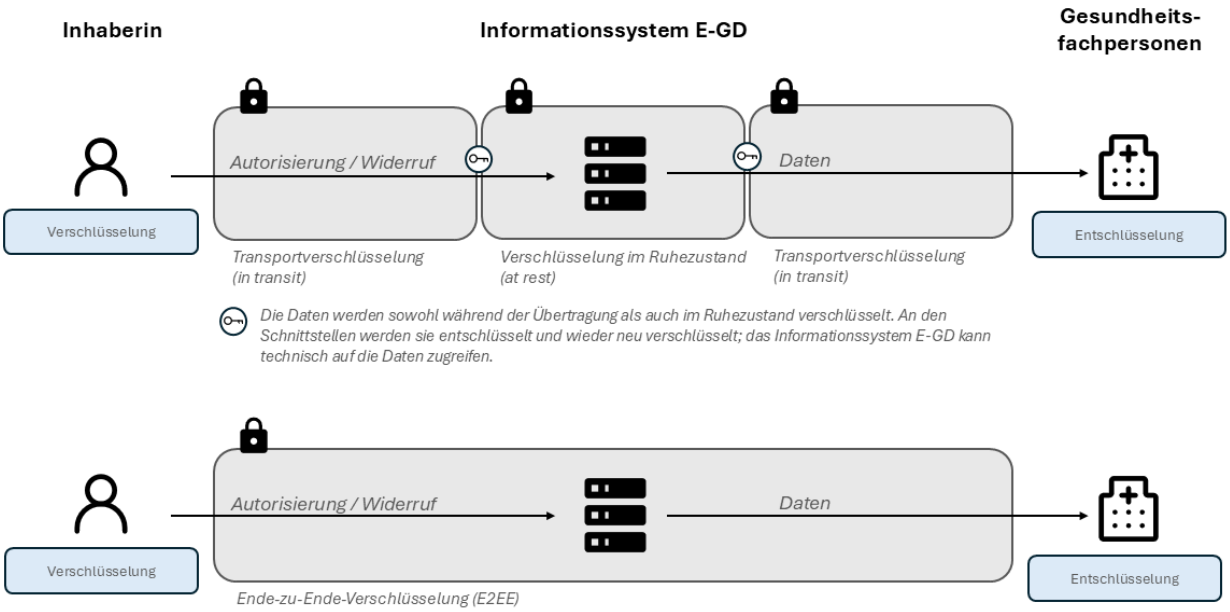
Im Rahmen einer Partnerschaft mit dem BAG hat das Center for Digital Trust (C4DT) der ETH Lausanne (EPFL) vier Varianten möglicher Sicherheitsarchitekturen für das künftige elektronische Gesundheitsdossier erarbeitet (siehe Beilage). Der zur Verfügung stehende Zeitrahmen war angesichts der sehr hohen technischen und organisatorischen Komplexität der Materie eng bemessen, daher konzentrierten sich die Arbeiten auf Grobkonzepte mit Machbarkeitsanalyse. Auf die Entwicklung detaillierter Sicherheitsarchitekturen wurde verzichtet, im Zentrum der Analyse stand die Bewertung der Implikationen der verschiedenen Varianten auf zentrale funktionale und regulatorische Systemelemente, namentlich Benutzerfreundlichkeit, Schlüsselmanagement, Systemkomplexität (= Kosten) und langfristige Weiterentwicklungsfähigkeit.

Die erste Variante skizziert eine primär organisatorisch abgestützte Lösung, bei welcher die Daten zwar nach aktuellem Stand der Technik verschlüsselt werden, die Betreiberin des E-GD rein technisch Zugriff auf die Daten hätte und der Schutz daher insbesondere durch organisatorische Massnahmen, Rechtskonformität und Vertrauen in die Betreiberin gewährleistet wird. Technisch anspruchsvoller ist Variante II. Sie stellt ein hybrides Modell vor, das Confidential Computing[1] nutzt und bei dem die Schlüssel in einem Vertrauensraum gespeichert werden. Die Varianten III und IV beschreiben Modelle mit strikter E2EE, die auf eine Schlüsselverwaltung durch die Inhaberinnen und Inhaber selbst bzw. vollständig dezentral durch verteilte vertrauenswürdige Instanzen setzen.

---

[1] Confidential Computing ist ein Sicherheitskonzept, das Daten nicht nur während der Übertragung, sondern auch während ihrer Verarbeitung schützt. Dabei kommen hardwarebasierte vertrauenswürdige Ausführungsumgebungen (Trusted Execution Environments, TEEs) zum Einsatz, um Datenbearbeitungen vom Rest des Systems zu isolieren.
Dies verhindert, dass etwa Betreiberinnen einer Infrastruktur, deren Administratoren oder Schadsoftware während der Verarbeitung auf sensible Daten zugreifen können. Im Unterschied zur E2EE-Verschlüsselung können dadurch Datenbearbeitungen mit geschützten Daten durchgeführt und dabei trotzdem starke Datenschutzgarantien geboten werden. Der Ansatz wird häufig für sicheres Cloud Computing, für Gesundheitsdaten und im Finanzsektor eingesetzt.

Abbildung: Unterschiede Variante I (oben) gegenüber E2EE (unten)



Quelle: Adaptiert aus Analyse "Data Security in the Swiss Electronic Health Records (E-GD): Four possible architectures"; Imad Aad, Linus Gasser, JP Hubaux Center for Digital Trust (C4DT), EPFL; Juli 2026

Tabelle: Variantenübersicht

	Beschrieb	**Kryptografisches Vertrauen**	**Technologie-Reifegrad**[2]	**grösste Nachteile**
I	durchgehende Verschlüsselung und organisatorischer Schutz	niedrig	produktiv (sehr hoch 9)	ist auf organisatorische Sicherheitsmassnahmen angewiesen
II	Verschlüsselung durch Confidential Computing	mittel	Funktionstüchtigkeit nachgewiesen (hoch, 8)	Hohe Komplexität und Abhängigkeiten: Am Markt erfüllen nur wenige Hardwarekomponenten die Anforderungen
III	Verschlüsselung und Schlüsselmanagement bei den Benutzenden	mittel	Prototyp (mittel, 6-7)	Infrastruktur sowie Schlüsselwiederherstellung liegen vollständig in der Verantwortung der Nutzenden – ohne institutionelle Absicherung.
IV	Vollständig dezentrale Schlüsselverwaltung	stark	Versuchsaufbau (rudimentär, 4-5)	Fehlende Standardisierung; lediglich experimentelle Umsetzungen ohne Produktionsreife bekannt

Quelle: Analyse "Data Security in the Swiss Electronic Health Records (E-GD): Four possible architectures"; Imad Aad, Linus Gasser, JP Hubaux Center for Digital Trust (C4DT), EPFL; Juli 2026

Die Ergebnisse zeigen zunächst, dass nicht alle Varianten der obenerwähnten engen Definition von E2EE entsprechen und bei E2EE auch verschiedene technische Ausprägungen existieren: Je nach gewählter Architektur unterscheiden sich die Implikationen für Sicherheit, Betrieb und Regulierung erheblich, weshalb eine pauschale Beurteilung der Verschlüsselungsmethode als solche

[2] Gemäss Skala Technology Readiness Level (TRL): www.sbfi.admin.ch > Forschung und Innovation; abgerufen am 10.07.2026

nicht sachgerecht erscheint. Mit zunehmender technischer Schutzwirkung der verschiedenen Architekturen nehmen das erreichte Datensicherheitsniveau, aber auch die Komplexität der Umsetzung und die Kosten zu. Gleichzeitig nehmen die Benutzerfreundlichkeit sowie der Reifegrad der erforderlichen Technologien ab.

Einschätzung und Zwischenfazit

Die Analyse macht deutlich, dass eine ausschliessliche Verwaltung der Schlüssel bei den Inhaberinnen und Inhaber (Variante III und IV) angesichts der damit verbundenen Anforderungen an die automatische Eröffnung, die Schlüsselwiederherstellung, den Notfallzugriff und die Kernfunktionen technische Herausforderungen mit sich bringt, die bislang nicht zufriedenstellend lösbar sind. Die Benutzerfreundlichkeit und der niederschwellige Zugang wären in der Umsetzung nicht gegeben. Der Bericht der EPFL unterstreicht zudem, dass diese Lösungen derzeit nur eine mittlere bis tiefe technische Maturität aufweisen – zu wenig für eine kritische Infrastruktur, die auf die ganze Schweiz skaliert werden soll, da sie noch nicht ausreichend erprobt, standardisiert und sich in realen Umgebungen im grossen Massstab bewährt haben. Insbesondere für die Umsetzung des Opt-Out-Modells existiert in diesen Varianten gegenwärtig auch international keine ausgereifte Lösung.

Demgegenüber erscheint der Einsatz einer hybriden Architektur (Variante II) mit Confidential Computing und einem Vertrauensraum unter bestimmten Voraussetzungen möglich. Allerdings fällt diese Lösung in einem eng definierten, technischen Begriffsverständnis nicht unter E2EE, könnte aber ein funktional gleichwertiges oder äquivalentes Schutzniveau erreichen. Doch auch bei dieser Variante erweist sich die konkrete architektonische Ausgestaltung als anspruchsvoll.

Die vorliegende Analyse der EPFL stellt eine erste grobe Einschätzung dar und weist hinsichtlich der Bewertungen zur Funktionalität, Betriebssicherheit sowie Skalierbarkeit noch Unschärfen auf. Weitere vertiefte Abklärungen sind unerlässlich und müssen insbesondere aufzeigen, ob die Funktionalitäten und die Benutzerfreundlichkeit bei der Umsetzung der Variante II sichergestellt werden können. Diese Variante verlangt teilweise nach speziellen Hardwarekomponenten etwa für den Vertrauensdatenraum, was Abhängigkeiten von einzelnen Herstellerinnen und relevante Kostensteigerungen für die Entwicklung und die laufenden Betriebskosten bedeuten könnte. Welche Variante schliesslich umsetzbar ist, muss zudem im Zusammenspiel mit übergeordneten Fragen diskutiert werden, dazu gehört auch das Zusammenspiel mit dem SwissHDS.

Wichtig ist erneut die Gesamtsicht: Sobald Daten den Verantwortungsbereich des E-GD-Systems verlassen, unterliegen sie fortan der technischen und organisatorischen Ausgestaltung der jeweiligen Primärsysteme, wo sie unter Umständen unverschlüsselt weiterbearbeitet werden. Technisch soll das E-GD nahtlos in den Gesundheitsdatenraum SwissHDS eingebunden sein. Das betrifft auch die Verschlüsselung. Nutzt das E-GD eine E2EE-Verschlüsselung, die nicht auf den ganzen Datenraum skaliert werden kann, werden Gesundheitsfachpersonen und Gesundheitseinrichtungen keine Daten aus dem E-GD nutzen. Auch ist zu befürchten, dass eine Ablage von Gesundheitsdaten im E-GD nicht erfolgt, weil die Bereitstellung im E-GD aufgrund der E2EE-Verschlüsselung als zu komplex oder aufwendig wahrgenommen wird. Patientinnen und Patienten würden dann – wie heute – sensible medizinische Informationen zum Beispiel unverschlüsselt per E-Mail an Gesundheitsfachpersonen senden. Für diesen Teil der Datenbearbeitung gelangen lediglich die allgemeinen Bestimmungen der Datenschutzgesetze des Bundes und (betreffend kantonalen Institutionen) der Kantone zur Anwendung.

Die vorliegenden Ergebnisse wurden auch mit dem BACS besprochen. Dieses weist dabei darauf hin, dass die beschriebenen Architekturmodelle insbesondere darauf fokussieren, Daten vor dem Zugriff durch die Betreiberin der E-GD-Infrastruktur zu schützen. Dieser Schutz erstreckt sich indes nur innerhalb des E-GD. Weiteren Angriffszielen, etwa einem grossen Datenabfluss z. B. den Missbrauch einer autorisierten Benutzerin, werden gemäss BACS dabei zu wenig Rechnung getragen, obwohl es mutmasslich das grösste Risiko für das E-GD darstellt. Dies sollte bei der Weiterentwicklung der Varianten stärker berücksichtigt werden.

Weiteres Vorgehen und Handlungsempfehlungen

Ausgestaltung der Sicherheitsarchitektur

Die Analyse der EPFL bietet im Rahmen der laufenden Arbeiten zur Sicherheitsarchitektur zusätzliche Anhaltspunkte. Entsprechend empfiehlt das BAG, diese Erkenntnisse weiter zu vertiefen und in das Detailkonzept einfliessen zu lassen. Im Rahmen dieser Arbeiten müssen Themen wie das Widerspruchsverfahren, der Notfallzugriff, die Vertretungen oder die Such- und Filterfunktionen vertieft analysiert werden und auf den flächendeckenden Einsatz ausgearbeitet und im Einzelnen allenfalls auch getestet werden. Themen wie Barrierefreiheit und digitale Inklusion sollen dabei ebenfalls aufgearbeitet werden. Bei der Ausgestaltung der Sicherheitsarchitektur des E-GD gilt es daher, ein ausgewogenes Verhältnis zwischen Sicherheit, Benutzerfreundlichkeit, Kosten und digitaler Souveränität zu finden. Eine einseitige Maximierung eines einzelnen dieser Ziele zulasten der übrigen würde weder der Praxistauglichkeit noch der Akzeptanz des Systems dienlich sein. Darüber hinaus muss neben einer hohen Maturität auch die Offenheit für künftige Entwicklungen gegeben sein: Die Systemarchitektur soll eine Abhängigkeit von einzelnen Anbietern oder spezifischen Technologien vermeiden. Die Integration künftiger Entwicklungen – etwa neuer Interoperabilitätsstandards, KI-gestützter Anwendungen oder veränderter Sicherheitsanforderungen etwa durch Entwicklungen im Bereich der Quantencomputer – muss jederzeit möglich sein. Schliesslich muss ebenfalls sichergestellt werden, dass ein kryptografisches Detailkonzept auch kompatibel mit dem SwissHDS ist.

Gesetzgeberische Erwägungen

Eine Verschlüsselung der Daten über die gesamte Bearbeitungskette entspricht dem heutigen Stand der Technik und ist für das E-GD so geplant. Der vorliegende Erlass des EGDG bietet daher eine hinreichende gesetzliche Grundlage für die Verschlüsselung der bearbeiteten Daten.[3] Ergänzend gelangen zudem die einschlägigen Bestimmungen anderer Erlasse zur Anwendung, namentlich das ISG und das DSG, welche ihrerseits Anforderungen an die Vertraulichkeit, Integrität und Verfügbarkeit der bearbeiteten Daten statuieren.

Es erscheint auch im Lichte des Berichts der EPFL nicht sachgerecht, für das E-GD ein konkretes kryptografisches Verfahren oder eine bestimmte Sicherheitsarchitektur – etwa E2EE in einer spezifischen Ausprägung – auf Gesetzesstufe festzuschreiben. Der Bundesrat hat sich bewusst für eine technologieneutrale Regelung entschieden, die dem Grundsatz Rechnung trägt, dass das Gesetz das «Was», also das zu erreichende Schutzniveau, verbindlich vorgibt, während die konkrete technische Umsetzung (das «Wie») im Ausführungsrecht sowie auf Vollzugsstufe erfolgt – etwa im Rahmen technischer Vorgaben von zu aktualisierenden Standards. Bei der Ausgestaltung des Ausführungsrechts werden interessierte Kreise in verschiedenen Gremien eingebunden und können sich ausserdem im Rahmen der Vernehmlassung einbringen. Zudem wird der Entwurf der entsprechenden Verordnung auf entsprechenden Wunsch hin selbstverständlich auch den zuständigen Kommissionen unterbreitet.

Dieser Ansatz ist in der schweizerischen Rechtsordnung etabliert, gerade im Bereich der Informationssicherheit und des Datenschutzes. Dabei wird meist auf im Einzelfall zu konkretisierende Begriffe wie «Stand der Technik» oder «angemessene technische und organisatorische Massnahmen» zurückgegriffen, um einerseits Rechtssicherheit hinsichtlich des angestrebten Schutzniveaus und andererseits die notwendige technische Flexibilität in Einklang zu bringen. So gibt es denn im Bundesrecht auf Gesetzesstufe bis anhin keine Vorgaben zu konkreten Verschlüsselungstechnologien. Dies zeigt sich auch bei aktuellen Gesetzgebungen, welche Verschlüsselungsfragen berühren: Sowohl das Bundesgesetz über die elektronische Identität und andere elektronische Nachweise (BGEID) als auch das Bundesgesetz über die Plattformen für die elektronische Kommunikation in der Justiz (BEKJ; SR 172.023) verzichten auf die Vorgabe konkreter kryptografischer Ver-

[3] Art. 5 Abs. 7 umfasst die Pflicht zur Gewährleistung eines angemessenen Schutzniveaus bei der Bearbeitung besonders schützenswerter Personendaten, ohne dabei ein bestimmtes technisches Verfahren vorzuschreiben; Art. 7 konkretisiert diese Schutzpflicht in Bezug auf die Datensicherheit und lässt damit hinreichend Raum für eine durchgehende Verschlüsselungsarchitektur.

fahren oder Standards und beschränken sich stattdessen auf die Formulierung technologieneutraler Schutzziele, deren Konkretisierung und Sicherstellung der Verordnungsstufe respektive dem Vollzug übertragen bleibt.

Sollte der kryptografische Schutz als allgemeine Anforderung explizit im Gesetz festgeschrieben werden, schlägt das BAG eine technologieneutrale Formulierung vor, die die konkrete Ausgestaltung beim E-GD offenlässt:

Ergänzung Artikel 5 Absatz 7

Der Bund ist für den Schutz und die Sicherheit der im Informationssystem E-GD enthaltenen Daten verantwortlich**, namentlich durch Verschlüsselung**. Er bewahrt die Daten nach schweizerischem Recht in der Schweiz auf.

So kann in enger Abstimmung mit bundesinternen Fachstellen und externen Sicherheitsexpertinnen und -experten konkretisiert und festgelegt werden, ob E2EE – und falls ja, in welcher Variante – eingesetzt werden soll. Damit wird nicht zuletzt sichergestellt, dass die konkrete Implementierung mit der fortschreitenden technischen Entwicklung Schritt halten und flexibel an künftige, ausgereifte Lösungen angepasst werden kann.