976/J
vom 05.06.2018 (XXVI.GP)

Anfrage

der Abgeordneten Stephanie Cox, Kolleginnen und Kollegen

an die Bundesministerin für Digitalisierung und Wirtschaftsstandort

betreffend „Digital Identity & strukturiertes Datenmanagement des Bundes“

BEGRÜNDUNG

Die überwältigenden Reaktionen der Medien auf den Datenskandal rund um das politische Beratungsunternehmen „Cambridge Analytica“, das sich auf dubiose Weise Daten von rund 87 Mio. Facebooknutzer_Innen aneignen konnte, zeigen, wie wenig Kontrolle jede/r Einzelne eigentliche über die eigenen Daten hat und was bereits wenige Leute mit solchen Daten anstellen können: Millionen Menschen gezielt manipulieren und ihr Verhalten steuern, oft mit falschen Informationen („Fake News“). Es werden sogar schon erste Stimmen laut, die fordern, dass Facebook seine „User“ für die Nutzung seiner Social Media-Plattform entschädigen soll, da Facebook mit den Userdaten viel Geld verdient. Die „User“, denen die Daten eigentlich gehören, gehen hingegen leer aus.

Datenskandale als Chance für Österreich

Österreich hat insofern gerade die große Chance eine Vorreiterrolle einzunehmen, als es seinen Bürger_Innen mehr bzw. vollständige Kontrolle über und Autonomie hinsichtlich ihrer Daten und damit ihrer (digitalen) Identität ermöglichen kann.
Im Regierungsprogramm findet sich in diesem Zusammenhang auch recht prominent das Pilotprojekt „Digitale Identität“. Geplant ist die „Einführung einer flächendeckenden sicheren digitalen Identität für einen sicheren und persönlichen Umgang mit den eigenen Daten“ mit dem Ziel, ein „einheitliches, staatlich gesichertes digitales Identitätsmanagementsystem als zentrale Basisinfrastruktur für die sichere Digitalisierung Österreichs“ zu schaffen. Betont wird das „Grundprinzip der Datenhoheit von Bürgern und Konsumenten“. Das neue System soll außerdem den „notwendigen Schutz vor Datenmissbrauch, Identitätsdiebstahl und Cyberkriminalität“ kombinieren, Bürger_Innen sollen ein Recht auf die Information haben, wer wann welche Daten genützt hat, und es soll ein „transparentes Verwendungsprotokoll der übermittelten Daten nur für die jeweiligen Bürger_Innen“ sichergestellt werden. Auch in der aktuellen 5G-Strategie wird die Datensouveränität erwähnt (S. 30).

Das Versprechen von „Self-Sovereign Identity“-Modellen

In den letzten Jahren bzw. Jahrzehnten konnte man eine schrittweise Weiterentwicklung des klassischen „Isolated Identity“-Modells (zum „Central“, zum „Federated“ und zum „User-Centric Identity Model“) beobachten. Die nächste Entwicklungsstufe stellt das „Self-Sovereign Identity“-Modell („SSI“) dar, das sich u.a. dadurch auszeichnet, dass:

- „User“ beliebig Attribute importieren oder entfernen können,

- „User" den Zugang zu ihren Daten kontrollieren können,
- Daten vollständig portabel sind,
- Datenintegrität sichergestellt werden kann (d.h. Daten können nicht manipuliert werden)
- kein Vertrauen in eine zentrale Autorität zur Generierung einer digitalen Identität sowie zur Datenverwaltung nötig ist.

Dieses SSI-Modell müsste man auch wählen, wenn man BürgerInnen tatsächlich volle Datenhoheit ermöglichen will. Durch die Umsetzung eines SSI-Modells, bei dem Daten dezentralisiert gespeichert werden, wären Daten auch sicherer vor Angriffen als bei der zentralen Speicherung von Daten. Mehr Transparenz würde auch das Vertrauen in die Politik bzw. den öffentlichen Sektor allgemein erhöhen. Außerdem würde die Einführung dieses Modells die Einhaltung der DSGVO für alle Stakeholder deutlich erleichtern (insb. im Hinblick auf Regelungen zu „explicit consent", Pseudonymisierung, dem Recht auf Richtigstellung und Löschung von Daten, sowie Datenportabilität).

Liest man sich das Konzept des SSI-Modells durch, bemerkt man schnell, dass „decentralized ledger" (bzw. „Blockchain") – vereinfacht gesprochen ein System zur Protokollierung von Datenübertragung – eine vielversprechende Technologie ist, um das SSI-Modell in die Realität umzusetzen. Im Whitepaper „about the Concept of Self-Sovereign Identity including its Potential"[1] kommt das "EGIZ" zum Schluss, dass "SOVRIN" – ein Open Source-Projekt, das u.a. ein „permissioned public distributed ledger"[2]-Modell sowie die Konzepte von „decentralized identifiers" („DIDs")[3] und „verifiable claims"[4] nützt – aktuell unter allen evaluierten Technologien für die Umsetzung des SSI-Konzepts am vielversprechendsten ist.

Zusammenhang zwischen „digitaler Identität" & anderen Digitalisierungsprojekten?

Im Regierungsprogramm liest man von einer Digitalisierungsoffensive, die neben dem bereits erwähnten Pilotprojekt „digitale Identität" auch „oesterreich.gv.at" – als „neue Bürger- und Unternehmensplattform", die ein „zentrales digitales Angebot für Serviceleistungen des Staates darstellen soll – umfasst. Zusätzlich will man „eHealth-Lösungen (z.B. ELGA)" ausbauen und ein "strukturiertes Datenmanagement des Bundes aufbauen", wobei bei letzterem Punkt ausdrücklich auf das estnische

[1] Siehe auch https://www.egiz.gv.at/files/download/Self-Sovereign-Identity-Whitepaper.pdf.

[2] „Permissioned public" bedeutet, dass zwar nur ausgewählte Akteure die „Blockchain" verwalten, dass diese jedoch von der Architektur für Jede/n offen ist. Dies erleichtert die Verwaltung, erhöht die Effizienz, ermöglicht einen größeren Schutz der Privatsphäre und netzwerkbezogene Probleme können einfacher gelöst werden.

[3] Mithilfe von „decentralized identifiers" („DIDs") können die Eigentümer einer digitalen Identität identifiziert werden. DIDs sind sozusagen der Schlüssel und „DID documents" sind der assoziierte Wert.

[4] Die Idee hinter „verifiable claims" ist, dass Jede/r bestimmte Attribute über jemand anderen behaupten kann. Kommen diese Behauptungen („claims") z.B. von einer staatlichen oder einer anderen Stelle (die/der „Issuer"), die hohes Vertrauen genießt, kann sich ein Dritter darauf verlassen, dass die Attribute wahr sind. So kann z.B. eine Universität einen Studienabschluss oder das Meldeamt eine Adresse nachweisen, ohne Aufschluss über sonstige Daten oder Informationen zu geben.

Modellprojekt „X-Road“ Bezug genommen wird. Bei all diesen Plänen, den komplexen technologischen Herausforderungen in der Planung und Umsetzung und dem ambitionierten Zeitplan ist oft nicht ganz klar, was eigentlich hinter den Begriffen „digitale Identität“, „oesterreich.gv.at“ oder „strukturiertes Datenmanagement des Bundes“ steht und wie diese Projekte zusammenhängen.

Die unterfertigenden Abgeordneten stellen daher folgende

Anfrage

1. Welches Identitätsmanagement-Modell (z.B. „Federated”, „User-Centric“, „Self-Sovereign“) plant Ihr Ministerium, mit dem Pilotprojekt „Digitale Identität“ umzusetzen? (Bitte auch um Angabe Ihrer konkreten Definition des jeweiligen Modells sowie einer Erläuterung, wieso das entsprechende Modell gewählt wurde und nicht ein anderes. Dies insbesondere, falls kein „Self-Sovereign“-Modell gewählt wird.)

2. Werden Sie bei der Umsetzung des Pilotprojekts „Digitale Identität“ eine technische Lösung wählen, bei der Daten der Bürger_Innen zentralisiert gespeichert werden oder werden Sie einen dezentralisierten Ansatz der Datenspeicherung verfolgen?
    a. Falls Sie einen zentralisierten Ansatz wählen, welche Vorteile und welche Nachteile sehen Sie im Vergleich zu einem dezentralisierten Ansatz?
    b. Falls Sie einen zentralisierten Ansatz wählen, wie werden Sie sicherstellen, dass Aktivitäten von Bürger_Innen nicht von einer zentralen Stelle eingesehen werden können?
        i. Falls Sie nicht verhindern werden, dass Aktivitäten von Bürger_Innen von einer zentralen Stelle eingesehen werden können, wieso nicht?
    c. Was ist Ihre Meinung zu Applikationen wie insb. SOVRIN, Blockstack, oder uPort, die bereits Projekte mit anderen Regierungen umsetzen und die Vorteile von „decentralized ledgers“ für ihre Identitätsmanagementsysteme nützen?

3. Sollte ein zentralisierter Ansatz gewählt werden, schließt dies nicht aus, dass Bürger_Innen auch andere Identitätsmanagementsysteme verwenden könnten, die z.B. „verifiable claims“ und „DIDs“ nützen. Wird Ihr Ministerium und/oder die Regierung konkrete Maßnahmen ergreifen, um die Nutzung von „Self-Sovereign-Identity-Lösungen“ (z.B. „SOVRIN“) zu unterstützen bzw. die geplante „eID“ mit solchen Tools zu verbinden?
(Finnland testet beispielsweise mit dem Projekt „TrustNet“ die Verbindung der finnischen eID mit SOVRIN. Ein ähnliches Projekt gibt es in der Schweizer Stadt „Zug“ mit „uPort“. Kanada hat mit „TheOrgBook“ ein digitales Firmenregister aufgebaut, in dem die Provinz British Columbia als „Issuer“ von „verifiable claims“ für Unternehmen auftritt. In Spanien plant das Konsortium „Alastria“ den Aufbau eines Nationalen „Blockchain Ecosystems“ mit einem Fokus auf „SSI“, „DIDs“ und „verifiable claims“, und Illinois (USA) setzt ein Pilotprojekt zu digitalen Geburtsurkunden um. Auch in Österreich gibt es

bereits starke Kompetenzen und konkrete Initiativen mit „Self-Sovereign Identity" Technologien.)

a. Falls ja, welche Maßnahmen sollen ergriffen werden und bis wann?
b. Falls nein, wieso nicht?
c. Wie bewerten Sie die oben angeführten Projekte in anderen Ländern?

4. Wie gedenkt Ihr Ministerium (bzw. die Regierung) die Anforderungen in der Wirtschaft hinsichtlich eines vertrauensbasierten Ökosystems auf Basis von „Self-Sovereign Identity" zu erfüllen, um in der Digitalisierung eine Chance gegen die diesbezüglichen Ansätze der großen, amerikanischen Plattformbetreiber zu haben? Wie erfolgt derzeit die Abstimmung bzw. Zusammenarbeit mit der Wirtschaft zu diesem Thema?

5. Welche Pilotprojekte wurden bereits bzw. werden derzeit – gem. § 25 Abs. 2 E-GovG) – durchgeführt, um das Projekt „Digitale Identität" zu testen?
   a. Wie wurde bzw. wird die Technologie im Rahmen des Pilotbetriebs bzw. der Pilotbetriebe konkret getestet?
   b. Welche Zeitpläne (inkl. „Milestones") gibt es für die aktuellen und künftig geplanten Projekte?
   c. Wie viele Personen waren bzw. sind als „Test-User" an den jeweiligen Projekten beteiligt?
   d. Wie wurden bzw. werden diese Projekte evaluiert?
   e. Was sind die Ergebnisse dieser Evaluierung?
   f. Welche Konsequenzen bzw. Maßnahmen ergeben sich aus der Evaluierung (z.B. Pilotierung einer neuen Technologie oder Überarbeitung konkreter Schwachstellen der bereits pilotierten Technologie)?

   (Bitte um abschließende Aufzählung aller Pilotprojekte und die Beantwortung der Fragen a. bis e. getrennt für jedes Projekt.)

6. Wurden alle Leistungen, die im Zusammenhang mit der Implementierung des Projektes „Digitale Identität" stehen, öffentlich ausgeschrieben?
   a. Falls ja, bitte um Auflistung aller Organisationen, der Leistungen bzw. Technologien, sowie Datum/Zeitraum.
   b. Falls nein, wieso nicht?
   c. Falls nein, mit welchen Organisationen wird bzw. wurde zusammengearbeitet, um das Projekt „Digitale Identität" zu implementieren (z.B. Softwarehersteller_Innen, Consultingdienstleister_Innen)? (Bitte um Auflistung aller beteiligten Organisationen, der Leistungen sowie Datum/Zeitraum.)

7. Wurde bzw. wird auf eine bereits bestehende technische Lösung zurückgegriffen oder wurde bzw. wird eine neue Lösung geschaffen?
   a. Falls nicht auf bestehende technische Lösungen zurückgegriffen wurde bzw. wird, wieso nicht?
   b. Falls nicht auf bestehende technische Lösungen zurückgegriffen wurde bzw. wird, welche bestehenden Lösungen wurden evaluiert und verglichen?
   c. Falls bestehende Lösungen um neue Technologien bzw. Lösungen erweitert wurden oder werden, um welche?

8. Wie bzw. aus welchen Mitteln wurde bzw. wird die Herstellung und Implementierung dieses Pilotprojekts finanziert? (Bitte um abschließende Auflistung aller bereits angefallenen Kosten je beteiligter Organisation sowie entsprechende Angabe der erbrachten Leistung und des Zeitraums der Leistungserbringung. Bitte überdies um Angabe der realistischerweise zu erwartenden Kosten).

9. In welchem Zusammenhang steht das Pilotprojekt „Digitale Identität" mit der Plattform „oesterreich.gv.at"? (Bitte um möglichst abschließende Erläuterung der unterschiedlichen Funktionen sowie um „Use Cases", die das Verhältnis beider Projekte deutlich machen.)

10. In welchem Zusammenhang steht das Pilotprojekt „Digitale Identität" mit dem geplanten strukturierten Datenmanagement des Bundes? (Bitte um möglichst abschließende Erläuterung der unterschiedlichen Funktionen sowie um „Use Cases", die das Verhältnis beider Projekte deutlich machen.)

11. In welchem Zusammenhang steht die Plattform „oesterreich.gv.at" mit dem geplanten strukturierten Datenmanagement des Bundes? (Bitte um möglichst abschließende Erläuterung der unterschiedlichen Funktionen sowie um „Use Cases", die das Verhältnis beider Projekte deutlich machen.)

12. Welche Technologie(n) soll(en) für die Implementierung des strukturierten Datenmanagements des Bundes verwendet werden? Ist beispielsweise, angesichts der Erwähnung im Regierungsprogramm, geplant, das estnische Modell zu verwenden d.h. die Interoperabilitätsplattform „X-Road" zusammen mit der „KSI-Blockchain", als Signaturservice? Bitte um abschließende und möglichst konkrete Erläuterung der Technologien, samt wesentlicher Funktionen und Eigenschaften, die verwendet werden sollen.
    a. Falls das estnische Modell (siehe oben) nicht als allgemeine Lösung in Österreich umgesetzt werden soll, wieso nicht?
    b. Falls zur Protokollierung von Datenübertragungen keine Lösung verwendet wird, die auf Blockchain-Basis funktioniert, wie stellen Sie a) die Integrität der Daten bzw. der Datenprotokollierung sowie b) die Transparenz des Abrufs bzw. der Verwendung solcher Daten (technisch) sicher? (Bitte um getrennte Beantwortung der Punkte a) und b).)
    a. Welche Register sollen durch die Einführung bzw. Erweiterung des strukturierten Datenmanagements des Bundes „geöffnet"[5] werden, um Datenübertragungen zu ermöglichen bzw. zu erleichtern? (Bitte um abschließende Auflistung aller Register, die nach derzeitiger Planung „geöffnet" werden sollen, sowie der Art und Funktionen der Schnittstellen.)
    b. Ist, abgesehen von Registern, auch geplant, andere Datenbanken von Ministerien im Rahmen der Einführung bzw. Erweiterung des strukturierten Datenmanagements des Bundes zu „öffnen", um z.B.

[5] Mit der Verwendung des Begriffs „geöffnet" ist ganz allgemein die Anbindung von Registern und (anderen) Datenbanken an das strukturelle Datenmanagementsystem des Bundes, etwa durch Schnittstellen, gemeint, um Datenübertragungen zwischen Organisationen (z.B. Ministerien) zu ermöglichen bzw. zu erleichtern.

Informations-/Datasilos – die zu Lasten der Effizienz in der Verwaltung gehen – vollständig zu eliminieren?

i. Falls ja, welche Datenbanken welcher Ministerien sollen „geöffnet" werden, um Datenübertragungen zu ermöglichen? (Bitte um abschließende Auflistung aller Datenbanken je Ministerium, die nach derzeitiger Planung „geöffnet" werden sollen, sowie der Art und Funktionen der Schnittstellen.)
ii. Falls nein, wieso nicht und welche Datenbanken sollen weiterhin isoliert bestehen? (Bitte um abschließende Auflistung aller Datenbanken je Ministerium, die nach derzeitiger Planung nicht „geöffnet" werden sollen.)
iii. Ist das Amtsgeheimnis – in der bestehenden Form – Ihrer Meinung nach a) ein nennenswerter Faktor, der zur Bildung von Informations-/Datasilos führt bzw. diese aufrechterhält, b) ein nennenswertes Hindernis für die weitere Effizienzsteigerung in der öffentlichen Verwaltung (insb. für den Aufbau des strukturierten Datenmanagements des Bundes). (Bitte um getrennte Antwort zu den Punkten a) und b).)

13. Soll das estnische Modell für den Ausbau von eHealth-Lösungen (z.B. ELGA) gewählt werden? (Insb. „X-Road" oder eine vergleichbare Lösung, als Technologie, die Krankenhäuser und andere Krankeneinrichtungen verbindet, um z.B. „e-prescriptions" nach estnischem Vorbild zu ermöglichen; die Verwendung der KSI-Blockchain oder einer vergleichbaren Lösung, um die Integrität sowie die Transparenz der Verwendung solcher Daten (technisch) sicherzustellen.)
    a. Falls nein, welche Technologien sollen für den Ausbau von eHealth-Lösungen gewählt werden?
    b. Falls nein, wie will man künftig a) die Datenintegrität von Gesundheitsdaten sowie b) die Transparenz des Abrufs bzw. der Verwendung solcher Daten (technisch) sicherstellen? (Bitte um getrennte Beantwortung der Punkte a) und b).)
    c. Sollen Daten zentralisiert gespeichert werden?
        i. Falls ja, welche Daten sollen zentralisiert gespeichert werden?
        ii. Falls ja, wie will man die Sicherheit dieser (sensiblen) Daten garantieren? (Dies insbesondere im Hinblick darauf, dass zentralisierte Datenspeicherung einen Angriff auf die jeweilige Datenbank attraktiver macht, da alle Daten – im Gegensatz zur dezentralisierten Datenspeicherung – an einem Ort sind.)
        iii. Wie will man generell – vor allem jedoch im Falle der zentralisierten Speicherung von Daten – sicherstellen, dass Daten (insb. Informationen zur Medikation von Personen), im Falle eines erfolgreichen Angriffs, nicht verwendet werden können, um auf den Gesundheitszustand bestimmter Personen zu schließen? (Anmerkung: Werden Medikamente verschrieben, ist es – z.B. durch Erhebung und Auswertung zusätzlicher (Meta-)Daten – grundsätzlich möglich, Medikationen bestimmten Personen zuzuordnen, wodurch Rückschlüsse auf die spezifische Krankheit bestimmter Personen möglich sind. Diese Problematik lässt sich durch reine Pseudonymisierung nie

ausschließen, vor allem nicht in Zeiten voranschreitender Digitalisierung.)

d. Welche technologische Lösung wird derzeit in der Steiermark verwendet, um das System, das unter dem Stichwort „e-Medikation" bekannt ist, zu ermöglichen und wie funktioniert diese? (Bitte auch um Erläuterung der wesentlichen Funktionen und Eigenschaften des Systems, insb. in Bezug auf die Frage 12.)
    i. Falls Daten zentralisiert gespeichert werden, um welche Daten handelt es sich?
    ii. Falls Daten zentralisiert gespeichert werden, wie will man die Sicherheit dieser (sensiblen) Daten garantieren? (Dies insb. im Hinblick darauf, dass zentralisierte Datenspeicherung einen Angriff auf die jeweilige Datenbank attraktiver macht, da alle Daten – im Gegensatz zur dezentralisierten Datenspeicherung – an einem Ort sind.)
    iii. Wie will man generell – vor allem jedoch im Falle der zentralisierten Speicherung von Daten – sicherstellen, dass Daten (insb. Informationen zur Medikation von Personen), im Falle eines erfolgreichen Angriffs, nicht verwendet werden können, um auf den Gesundheitszustand bestimmter Personen zu schließen? (siehe auch Frage 13.c.iii.)

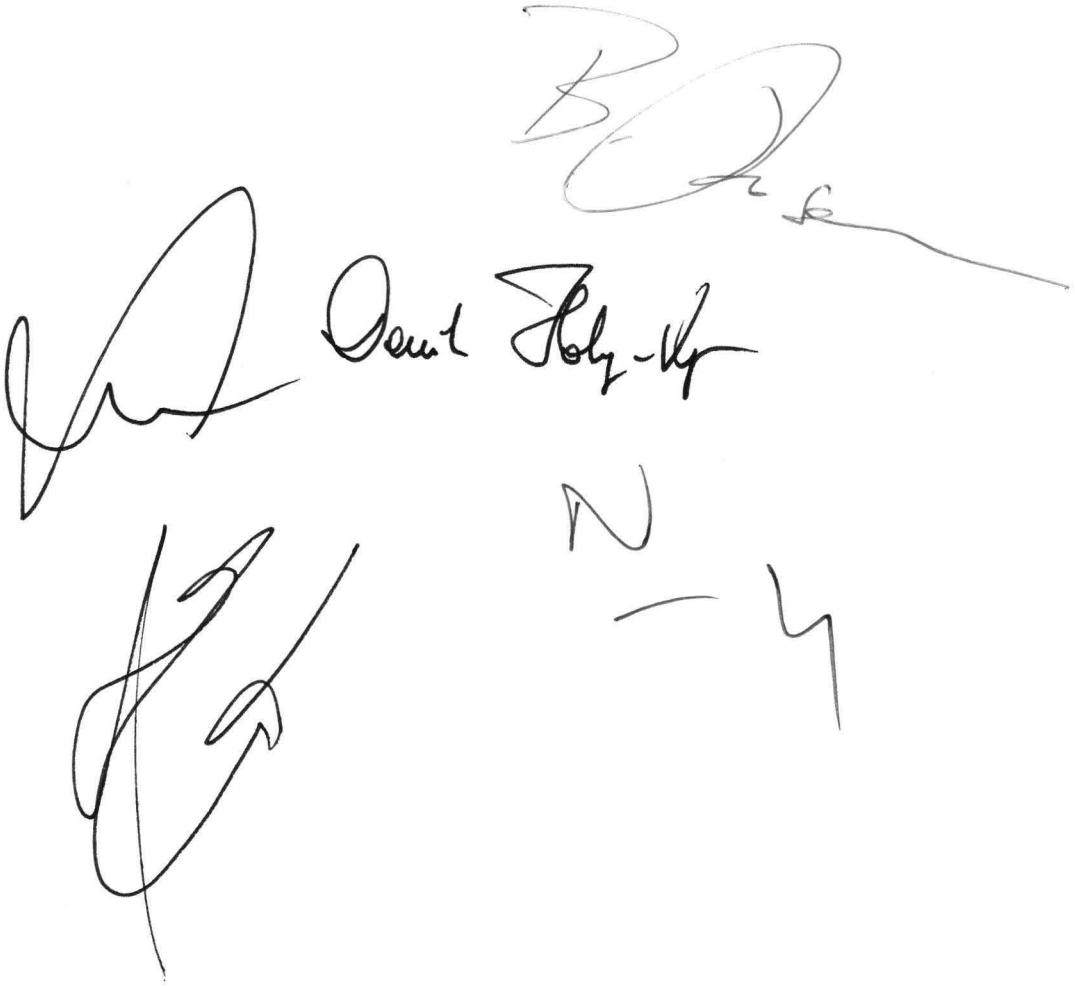
14. Wurden alle Leistungen, die im Zusammenhang mit der Implementierung des strukturierten Datenmanagements des Bundes (inkl. der eHealth-Lösungen) stehen, öffentlich ausgeschrieben?
    a. Falls ja, bitte um Auflistung aller Organisationen, der Leistungen bzw. Technologien, sowie Datum/Zeitraum.
    b. Falls nein, wieso nicht?
    c. Falls nein, mit welchen Organisationen wird bzw. wurde zusammengearbeitet, um das Projekt „Digitale Identität" zu implementieren (z.B. Softwarehersteller_Innen, Consultingdienstleister_Innen)? (Bitte um Auflistung aller beteiligten Organisationen, der Leistungen sowie Datum/Zeitraum.)

15. Wurde bzw. wird zur Umsetzung des strukturierten Datenmanagements (inkl. der eHealth-Lösungen) auf eine bereits bestehende technische Lösung zurückgegriffen oder wurde bzw. wird eine neue Lösung geschaffen?
    a. Falls nicht auf bestehende technische Lösungen zurückgegriffen wurde bzw. wird, wieso nicht?
    b. Falls nicht auf bestehende technische Lösungen zurückgegriffen wurde bzw. wird, welche bestehenden Lösungen wurden evaluiert und verglichen?
    c. Falls bestehende Lösungen, um neue Technologien bzw. Lösungen erweitert wurden oder werden, um welche?

16. Wie bzw. aus welchen Mitteln wurde bzw. wird die Herstellung und Implementierung des strukturierten Datenmanagements (inkl. der eHealth-Lösungen) des Bundes finanziert? (Bitte um abschließende Auflistung aller bereits angefallenen Kosten je beteiligter Organisation sowie entsprechende Angabe der erbrachten Leistung und des Zeitraums der Leistungserbringung. Bitte überdies um Angabe der realistischerweise zu erwartenden Kosten).

17. Werden Ihrer Meinung nach Änderungen der geltenden Rechtslage nötig sein, um die Projekte i) „Digitale Identität“, ii) „oesterreich.gv.at“, iii) „strukturiertes Datenmanagement des Bundes“ (inkl. der eHealth-Lösungen) zu ermöglichen?
    a. Falls ja, welche Rechtsänderungen halten Sie künftig für nötig und wieso?
    b. Falls nein, wieso nicht?

    (Bitte um Beantwortung der Fragen a. und b. jeweils getrennt für die Punkte i), ii) und iii).



REPUBLIK ÖSTERREICH Parlamentsdirektion SIEGEL	**Unterzeichner**	Parlamentsdirektion
	Datum/Zeit-UTC	2018-06-05T16:32:09+02:00
	Prüfinformation	Informationen zur Prüfung des elektronischen Siegels und des Ausdrucks finden Sie unter: https://www.parlament.gv.at/siegel
Hinweis	Dieses Dokument wurde elektronisch besiegelt.	