AWK Group
Enabling digital performance.

Umsetzungsziel 13 der E-Government Strategie Schweiz 2020-2023

Machbarkeitsstudie zur Nachvollziehbarkeit der Verwendung persönlicher Daten

Auftraggeber:
Geschäftsstelle E-Government Schweiz
Haus der Kantone
Speichergasse 6
3003 Bern

Dezember 2021

Dokumentinformationen

Titel:	Machbarkeitsstudie zur Nachvollziehbarkeit der Verwendung persönlicher Daten
Projektnummer:	Umsetzungsziel 13 der E-Government Strategie Schweiz 2020-2023
Abschluss der Studie:	Dezember 2021
Gespeichert:	12. Dezember 2021
Anzahl Seiten:	105
Dateiname:	Ber_Machbarkeitsstudie_UZ13_v1-0
Dokumentverantwortlicher:	Dominik Bischoff
Geprüft durch:	Projektbegleiter: Andreas Meier

Versionen

Version	Datum	Wichtigste Änderungen	Verantwortlich
V 0.1	2021	Review einzelner Kapitel durch den Fachausschuss	Dominik Bischoff, Andreas Meier
V 0.9	28.10.2021	Erste komplette Version – Versand an Fachausschuss sowie weitere Stakeholder zum Review	Dominik Bischoff, Andreas Meier
V 1.0	08.12.2021	Finale Version inklusive Feedback von Fachausschuss	Dominik Bischoff, Andreas Meier

Abkürzungen und Begriffe

Abkürzung	Beschreibung
clickable Mockup	Eine simulierte Nachvollziehbarkeitslösung ohne echte Funktionalität und Daten, welche gemeinsam mit natürlichen Personen getestet werden kann
DSG	Datenschutzgesetz
Nachvollziehbarkeit	Nachvollziehbarkeit der Verwendung von Personendaten durch die öffentliche Verwaltung
Nachvollziehbarkeitslösung	Eine oder mehrere Lösungen, welche natürlichen Personen die für die Nachvollziehbarkeit notwendigen Informationen bereitstellt.
POC	Proof of Concept
Quellsystem	Sammelbegriff für sämtliche Systeme verwendet, welche an eine Nachvollziehbarkeitslösung angeschlossen werden könnten.
UZ13	Umsetzungsziel 13

Inhaltsverzeichnis

1. Management Summary

Durch Transparenz Vertrauen schaffen

Vertrauen in die öffentliche Verwaltung ist eine wichtige Voraussetzung dafür, dass diese ihre Aufgaben gut erfüllen kann. Fehlt das Vertrauen der natürlichen Personen in Ihre Verwaltung, so erschwert sich deren Weiterentwicklung, indem das Stimmvolk im Zweifelsfall «Nein» zu Vorhaben der digitalen Transformation stimmt.

Es gibt verschiedenste Massnahmen, mit welchen die öffentlichen Verwaltungen der verschiedenen Staatsebenen Vertrauen schaffen können. Freiwillige Transparenz der öffentlichen Verwaltungen schafft im Allgemeinen und auf lange Sicht Vertrauen. Eine möglichst transparente öffentliche Verwaltung erlaubt es Personen nachzuprüfen, ob die Verwaltung ihre Aufgaben gemäss den aufgetragenen Vorgaben ausführt.

Im Vergleich zu umliegenden EU-Ländern hat die öffentliche Verwaltung der Schweiz gemäss der EU-Benchmarkstudie Nachholbedarf im Bereich der Transparenz von digitalen Dienstleistungen (E-Government). Unter anderem im Umgang der öffentlichen Verwaltung mit Personendaten wurde Potenzial für mehr Transparenz identifiziert.

Vision von mehr Transparenz im Umgang der öffentlichen Verwaltung mit Personendaten

Die vorliegende Machbarkeitsstudie ist das Resultat des Umsetzungsziels 13 der E-Government-Strategie Schweiz 2020–2023. Durch Schaffung von Transparenz in der Verwendung von Personendaten soll das Vertrauen von natürlichen Personen in die öffentliche Verwaltung gesteigert werden. Die Studie fokussiert darauf, wie dieser Mehrwert zusätzlicher Transparenz für natürliche Personen geschaffen werden könnte.

Konkret wird untersucht, inwiefern die öffentliche Verwaltung natürlichen Personen Einsicht in folgende Fragestellungen oder Teilaspekte davon geben könnte:

- In welchen Systemen der öffentlichen Verwaltung sind von der betroffenen natürlichen Person Daten gespeichert?
- Welche Organisationseinheiten der öffentlichen Verwaltung dürfen auf welche Personendaten zugreifen? In welchen Systemen werden diese gespeichert und verarbeitet? Wie sehen die Datenflüsse zwischen den Systemen aus?
- Welche Organisationseinheit der öffentlichen Verwaltung hat wann und aus welchem Grund Einsicht in welche Personendaten der betroffenen Person gehabt?
- Wie sieht der Inhalt der gespeicherten Personendaten der betroffenen Person aus?

Die digitale Lösung, welche natürlichen Personen Antworten auf diese Fragestellungen geben soll, wird im Folgenden «Nachvollziehbarkeitslösung» genannt. Eine solche «Nachvollziehbarkeitslösung» muss in keiner Weise ein zentrales System sein, sondern kann genauso aus mehreren föderierten oder dezentralen Systemen bestehen.

Explizit nicht im Umfang einer möglichen Nachvollziehbarkeitslösung sind die Möglichkeit der Korrektur von fehlerhaften Daten durch die betroffene natürliche Person oder die Freigabe von Personendaten an bisher nicht berechtigte Verwaltungseinheiten. Die Analyse der Rechtsgrundlagen wird basierend auf den Resultaten dieser Machbarkeitsstudie in einem separaten Dokument publiziert.

Der Bedarf der natürlichen Personen nach Transparenz

Verschiedene Studien haben exemplarisch aufgezeigt, dass Transparenz und das Gefühl von Kontrolle über die eigenen Daten wichtige Bedingungen für die Akzeptanz von digitalen Dienstleistungen der öffentlichen Verwaltung durch natürliche Personen sind. Ein grundsätzlicher Bedarf von natürlichen Personen nach zusätzlicher Transparenz der öffentlichen Verwaltung im Umgang mit Personendaten ist folglich vorhanden. Im Detail ist davon auszugehen, dass sich dieser Bedarf von Person zu Person unterscheidet. Für ein mögliches zukünftiges Nachvollziehbarkeitssystem bedeutet dies, dass im Rahmen der Konzeption vertiefte Abklärungen darüber notwendig sind, welche Informationen und Funktionalitäten für natürliche Personen im Bereich der Transparenz der Personendaten den grössten Mehrwert bieten.

Hohe Transparenz ist aktuell nur in der Theorie vorhanden

Die Aufgaben der öffentlichen Verwaltung sind gemäss Legalitätsprinzip durch rechtliche Grundlagen beschrieben. Dies bedeutet, dass jede erlaubte Aktion auf Personendaten durch die öffentlichen Verwaltungen in einer öffentlich einsehbaren rechtlichen Grundlage festgehalten ist. Der grosse Umfang und die Komplexität der rechtlichen Grundlagen erlaubt es natürlichen Personen jedoch kaum, daraus Transparenz über die Verwendung der eigenen Personendaten zu erlangen. Für natürliche Personen ist es heute daher nahezu unmöglich nachzuvollziehen, welche Verwaltungseinheit welche Personendaten über sie speichert und verwendet. Auch auf Seite der Verwaltung besteht aktuell keine vollständige Übersicht.

Mehrere tausend Systeme, in welchen Personendaten verarbeitet werden

Die Komplexität der System- und Prozesslandschaft, in welcher Personendaten durch die öffentliche Verwaltung bearbeitet werden, ist hoch. Es existieren heute mehrere tausend IT-Systeme in welchen Personendaten verarbeitet werden und eine noch grössere Anzahl von Datensammlungen. Diese Systeme sind über alle drei föderal organisierten Staatsebenen sowie verschiedene Fachbereiche (Finanzen, Sozialwesen, Gesundheitswesen, Mobilität, ...) verteilt. Die Verteilung von Personendaten auf verschiedene Systeme ist oftmals historisch gewachsen und wird teilweise von der Politik aktiv eingefordert.

Wichtige Enabler, welche die Umsetzung einer Nachvollziehbarkeitslösung unterstützen könnten, fehlen aktuell oder sind erst in der Erarbeitung. Solche Enabler sind beispielsweise eine national anerkannte E-ID, ein verwaltungsweit einheitliches Daten-Management, die Standardisierung und Harmonisierung von Daten in verschiedenen Systemen sowie eine breite Verwendung von einheitlichen Identifikatoren.

Die langfristige Vision einer umfassenden Nachvollziehbarkeitslösung

Als langfristige Vision kann der Zustand angestrebt werden, in welchem natürliche Personen bei Interesse die Verwendung ihrer Personendaten durch die öffentliche Verwaltung vollständig transparent nachvollziehen können. Hierzu müssten eine oder mehrere miteinander verbundene Nachvollziehbarkeitslösungen aufgebaut werden, welche eine grosse Anzahl von Quellsystemen mit den darin gepflegten Datensammlungen anbinden. Kurz- und mittelfristig ist eine solche skalierbare Nachvollziehbarkeitslösung aufgrund der hohen Gesamtkomplexität, der grossen Anzahl an Systemen und Datensammlungen sowie den aktuell fehlenden Enablern nur schwer umsetzbar.

Mit einem explorativen Vorgehen zum Ziel

Mit einem schrittweisen und explorativen Vorgehen können Fortschritte in Richtung dieser langfristigen Vision erzielt werden. Ein explorativ Vorgehen erlaubt es zudem, weitere Informationen über die Bedürfnisse der natürlichen Personen zu erhalten sowie diese in die Entwicklung eng einzubinden. Basierend auf der Diskussion des Lösungsraums wurden sinnvolle Varianten definiert. Diese müssen umsetzbar sein, akzeptiert werden und einen Schritt in Richtung der Vision gehen.

Der Fachausschuss von UZ13 empfiehlt, das Thema der Nachvollziehbarkeit der Verwendung von Personendaten durch die öffentliche Verwaltung im Rahmen der «Agenda Digitale Verwaltung Schweiz (DVS)» weiterzuverfolgen. Folgende vier Punkte werden zur Umsetzung empfohlen:

Empfehlung 1: Partner für einen Proof of Concept evaluieren

Eine Option für ein explorativ Vorgehen ist die Umsetzung einer eng eingegrenzten Nachvollziehbarkeitslösung mit nur einem oder wenigen angeschlossenen Quellsystemen. So können vertiefte Erfahrungen darüber gesammelt werden, ob und wie natürliche Personen eine Nachvollziehbarkeitslösung im täglichen Leben verwenden sowie darüber, wie diese systemseitig umgesetzt werden kann.

Der Ausgangspunkt für den Erfolg einer Nachvollziehbarkeitslösung ist die Erfüllung der Bedürfnisse der natürlichen Personen. Es wird daher empfohlen, im Rahmen des weiteren Vorgehens auf nutzerzentrierte Methoden wie beispielsweise die Erstellung eines Mockups zurückzugreifen, um die natürlichen Personen von Anfang an ins Zentrum der Lösung zu stellen.

Die Umsetzung eines Proof of Concepts erfolgt idealerweise in Zusammenarbeit mit einem oder mehreren Quellsystempartnern. Mögliche identifizierte Opportunitäten sind hierbei zentralisierte Quellsysteme (bspw. Nationaler Adressdienst, UID-Register, Infostar) oder kantonale E-Government Portale. Auch einfachere Quellsysteme können geeignete Kandidaten sein, sofern diese für natürliche Personen ausreichend interessant sind. Die Suche nach geeigneten Partnern kann sofort begonnen werden.

Dieses Vorgehen eines Nachvollziehbarkeitssystems mit wenigen angeschlossenen Quellsystemen wurde in Estland und Luxemburg erfolgreich umgesetzt und ist in Dänemark zur Umsetzung geplant. Im Vergleich zur Schweiz besteht in diesen Ländern jedoch eine höhere Zentralisierung von IT-Systemen und den darin gespeicherten Personendatensammlungen.

Im Rahmen dieser Machbarkeitsstudie wurden zudem Fragestellungen für die nationale E-Government Umfrage 2021 erarbeitet, welche zusätzliche Informationen zum Bedarf von natürlichen Personen nach zusätzlicher Transparenz und Nachvollziehbarkeit liefern sollen. Die Resultate werden Anfang 2022 zur Verfügung stehen.

Empfehlung 2: Die Arbeit an den Enablern fortsetzen

Die Arbeit an den verschiedenen Enablern soll fortgesetzt werden: Die Schaffung einer nationalen E-ID, ein verwaltungsweites Datenmanagement inklusive Standardisierung und Harmonisierung von Daten sowie die systemübergreifende Verwendung von eindeutigen Identifikatoren für natürliche Personen.

Empfehlung 3: Kommunikative Massnahmen zur Verbesserung der Transparenz umsetzen

Als Sofortmassnahme kann die Kommunikation zur Datenverwendung auf besonders relevanten Systemen verbessert werden. Mit geringem Aufwand kann mittels geeigneter Massnahmen wie beispielsweise Info-Grafiken oder Erklärvideos zusätzliche Transparenz gegenüber natürlichen Personen geschaffen werden. Ein zentraler Zusammenzug solcher Kommunikationsmassnahmen beispielsweise auf ch.ch ist zu prüfen.

Empfehlung 4: Das Thema der Nachvollziehbarkeit der Verwendung von Personendaten in der Verwaltung verankern

Mit dieser Machbarkeitsstudie wurde ein Schritt in Richtung einer Nachvollziehbarkeitslösung der Verwendung von Personendaten durch die öffentliche Verwaltung gemacht. Der Fachausschuss empfiehlt, dass die Digitale Verwaltung Schweiz (DVS) das Thema im Rahmen der Agenda DVS weiterverfolgt. Hierzu sollen in einem ersten Schritt die hier vorliegende Machbarkeitsstudie publiziert und bei den relevanten Stakeholdern bekannt gemacht werden. Diese sind bei Interesse in die Weiterentwicklung des Themas aktiv einzubinden.

2. Prolog: «Maria Müller» und die Daten ihrer Steuererklärung

Es ist der 13. April 2021: Maria Müller[1] hat im Online-Portal des Kantons Bern[2] ihre Steuererklärung eingereicht. Sie fragt sich, was jetzt eigentlich genau mit den Daten passiert, welche sie in die Online-Steuererklärung eingetippt hat. Sie erinnert sich daran, dass sie im letzten Jahr Bundes-, Kantons-, Gemeinde- und Kirchensteuern bezahlt hat. Sie geht also davon aus, dass verschiedene Verwaltungseinheiten Zugriff auf ihre persönlichen Daten haben, da sie ihre Steuererklärung ja lediglich beim Kanton einreicht. Doch wer hat Zugriff auf welche Daten?

- Bekommt ihre Kirchgemeinde (oder sogar die Landeskirche) die Information, dass sie ein Ferienhaus in Sion besitzt?
- Bekommt die Krankenversicherung die Information, dass sie Anrecht auf eine Prämienverbilligung hat?
- Sie hat zudem im Formular die Daten ihres neuen Kontos eingegeben. Muss Sie diese aktualisierte Information auch an weitere Verwaltungsstellen melden, oder geht das automatisch?
- Kann ihr Freund, welcher als Kantonspolizist arbeitet, ihre Steuerunterlagen einsehen?

Diese und ähnliche Fragen beschäftigen Maria Müller. Die Webseite, auf welcher Sie die Steuerunterlagen eingereicht hat, beantwortet ihre Fragen leider nicht ausreichend. Per Internet-Suche findet sie das Steuergesetz des Kantons Bern. Sie beginnt zu lesen, ist vom juristischen Deutsch und der Länge des Textes aber überfordert und gibt nach wenigen Minuten auf. Sie überlegt sich, ob sie der Steuerverwaltung einen Brief schreiben soll, um Antworten auf ihre Fragen zu bekommen. Sie entscheidet sich dagegen, da sie Angst hat, mit ihrem Brief gegenüber der Verwaltung als «mühsam» zu erscheinen.

Maria fragt sich, ob es in der heutigen digitalisierten Welt nicht möglich sein müsste, dass sie sich auf einer Website mit ihrem BE-Login einloggen kann und dann sieht, wer konkret auf ihre Steuerunterlagen des letzten Jahres zugegriffen hat? Und wenn Sie schon dabei ist, würde Maria auch interessieren, welche Daten die Verwaltung sonst noch von ihr besitzt.

[1] Fiktive Storyline – Ähnlichkeiten mit realen Personen sind rein zufällig.

[2] Exemplarisch für einen beliebigen Kanton mit Online-Steuererklärung. Es soll keine Bewertung gemacht werden, ob der Kanton Bern die Thematik besser oder schlechter als andere Kantone gelöst hat.

3. Ausgangslage

3.1. Das Umsetzungsziel 13 der E-Government Strategie 2020-2023

Der Bund, die Kantone und die Gemeinden definieren in der E-Government-Strategie Schweiz die gemeinsamen Ziele, welche sie für die digitale Transformation der öffentlichen Verwaltung definieren[3]. Im Rahmen der aktuell gültigen Strategie 2020-2023 wurde ein Umsetzungsplan[4] erarbeitet, in welchem vier strategische Ziele sowie 21 Umsetzungsziele definiert wurden.

Mit dem Umsetzungsziel 13 des überarbeiteten «Umsetzungsplan 2021–2023» wird eine Machbarkeitsstudie zur Nachvollziehbarkeit der Verwendung persönlicher Daten erarbeitet. Das Umsetzungsziel 13 ist Teil des strategischen Ziels «Wissen zur Digitalisierung der Verwaltung fördern und Vertrauen stärken». Im Sinne einer «HERMES-Studie» für die Initialisierungsphase wurden folgende Ziele für die vorliegende Machbarkeitsstudie definiert:

- Identifizierung des Bedarfs nach Nachvollziehbarkeit im Bereich der Verwendung persönlicher Daten, sowie des Nutzens einer entsprechenden Lösung
- Schaffung einer Entscheidungsgrundlage über die Durchführbarkeit eines potenziellen Umsetzungsprojektes
- Aufzeigen von Varianten sowie der dazugehörigen Chancen und Risiken
- Grobe Richtungsvorgabe für eine Durchführung und Umsetzung eines Projekts

Die Machbarkeitsstudie wurde durch die AWK Group AG im Zeitraum von Q4 2020 bis Q4 2021 in Zusammenarbeit mit dem Fachausschuss und dem Auftraggeber des Projekts erstellt. Weitere Informationen zum Vorgehen sowie zur Zusammensetzung des Fachausschusses sind in Anhang A.1 aufgeführt.

3.2. Der Begriff der Nachvollziehbarkeit

In dieser Machbarkeitsstudie wird der Begriff der Nachvollziehbarkeit verwendet. Damit sind Massnahmen gemeint, welche es natürlichen Personen erlauben, die Verwendung ihrer jeweiligen Personendaten durch die öffentliche Verwaltung besser nachzuvollziehen. Dadurch kann für natürliche Personen zusätzliche Transparenz darüber entstehen, wie ihre jeweiligen Personendaten durch die öffentliche Verwaltung zwecks Erfüllung ihrer Aufgaben verwendet werden. Dies jedoch nur dann, wenn eine natürliche Person auch aktiv die Informationen einsieht, welche durch die öffentliche Verwaltung in diesem Rahmen bereitgestellt werden.

Andere transparenzsteigernde Massnahmen – wie beispielsweise die Publikation von offenen Behördendaten («Open Government Data», OGD) oder auch von Dokumenten (Öffentlichkeitsprinzip) – sind damit explizit nicht gemeint. Die Nachvollziehbarkeit von Personendaten ist folglich eine Teilmenge sämtlicher Massnahmen der öffentlichen Verwaltung, welche die Transparenz fördern können. Dies ist in Abbildung 1 dargestellt.

Eine Lösung, welche es natürlichen Personen erlaubt, Nachvollziehbarkeit über die Verwendung ihrer Personendaten durch die öffentliche Verwaltung zu erlangen, wird im folgenden Nachvollziehbarkeitslösung genannt. Es wird der Einfachheit halber von «der Nachvollziehbarkeitslösung» gesprochen. Diese Begriffsverwendung bezeichnet das Gesamtsystem und soll explizit nicht aus-

[3] Siehe: https://www.egovernment.ch/de/umsetzung/e-government-strategie/

[4] Siehe: https://www.egovernment.ch/de/umsetzung/umsetzungsplan/

schliessen, dass dieses aus mehreren voneinander unabhängigen oder miteinander verknüpften Systemen bestehen könnte.

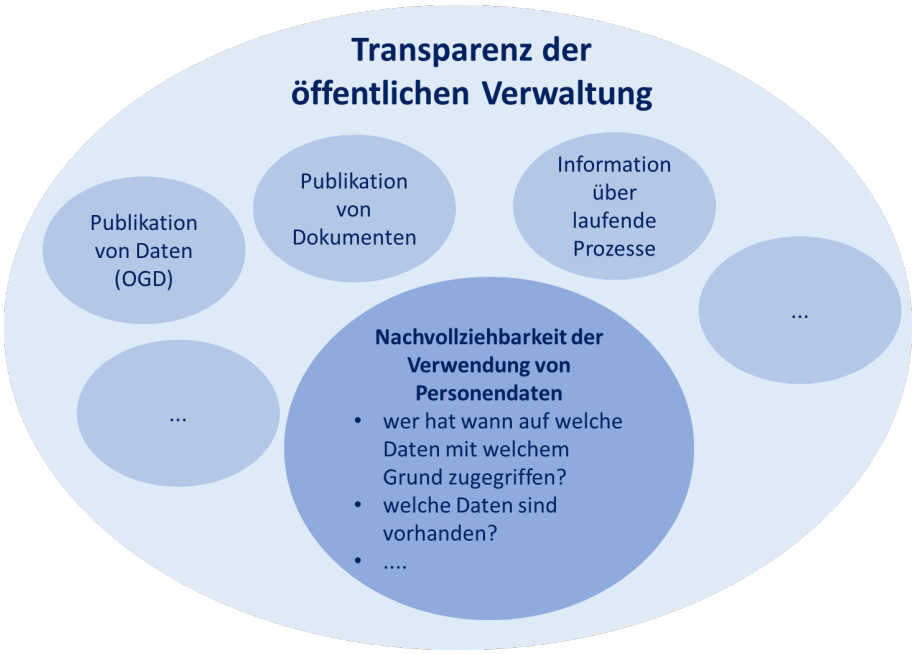

Abbildung 1: Die Begriffe der Transparenz und der Nachvollziehbarkeit.

3.3. Eingrenzung der Themen, welche im Umfang der Machbarkeitsstudie untersucht werden

Um ein gemeinsames Verständnis darüber zu erlangen, welches Ziel mit dem Vorhaben UZ13 erreicht werden soll, wurde gemeinsam mit dem Fachausschuss und dem Auftraggeber folgende Vision ausgearbeitet:

> **Durch Transparenz im Bereich der Datenhaltung und Datenverarbeitung das Vertrauen in die digitale Verwaltung stärken**

Basierend auf dieser Vision wurde dann zu Beginn der Studie im Rahmen der «Grobanalyse» evaluiert, wie der Umfang des Projektes «UZ13 Nachvollziehbarkeit der Verwendung von Personendaten» abgesteckt werden soll. Die detaillierte «Grobanalyse» ist in Anhang A.2 aufgeführt. Tabelle 1 zeigt die Themengebiete auf, welche untersucht wurden.

Tabelle 1: Unterteilung des Umfangs der Machbarkeitsstudie in Themengebiete

Themengebiet	Kapitel	Relevante Unterthemen				
Nutzende der Nachvollziehbarkeitslösung	A.2.1	Personen, welche von Nachvollziehbarkeitslösung profitieren sollen				
Auskunft über Daten, Verwendung und Weitergabe	A.2.2 - A.2.7	Welche Informationen über die Verwendung werden dem Nutzenden geben	Details zur Nutzung	Details zur Datenweitergabe	Details zu gespeicherten Daten	historischer Verlauf
Definition der nachvollziehbaren Personendaten	A.2.8	nachvollziehbare Personendaten				
Stufe bis zur welcher eine Nachvollziehbarkeit erfolgt	A.2.9	Nachvollziehbarkeit bis auf Stufe				
Anzustrebender Zusatznutzen für natürliche Personen	A.2.10	Zusatznutzen für nat. Personen				
Anzustrebender Zusatznutzen für öffentliche Verwaltung	A.2.11	Zusatznutzen für die Verwaltung				
Einzubindende Systeme	A.2.12 - A.2.15	In Nachvollziehbarkeitslösung einzubindende Systeme	In Nachvollziehbarkeitslösung einzubindende Partner	In Nachvollziehbarkeitslösung einzubindende System-Typen		

Generell wurde der mögliche Umfang relativ grosszügig ausgelegt, um bei der Ausgestaltung von Lösungsansätzen entsprechenden Handlungsspielraum zu haben. Folgende Liste zeigt zusammenfassend die wichtigsten Entscheidungen zur Eingrenzung des Vorhabens auf:

- Fokus auf natürliche Personen, welche regelmässigen Kontakt zu Schweizer Verwaltungseinheiten haben (i.e. müssen nicht zwingend Schweizer Bürger sein). Juristische Personen wurden explizit ausgeschlossen.

- Fokus auf eine grundsätzlich digitale Nachvollziehbarkeitslösung[5]
- Im maximalen «Funktionsumfang» könnten folgende Informationen für natürliche Personen zur Verfügung gestellt werden:
    - Einsicht in den Inhalt der Daten, welche über die betreffende natürliche Person durch die öffentliche Verwaltung gespeichert sind
    - Ausweisen, wann auf welche Personendaten der betroffenen natürlichen Person zugegriffen wurde
    - Ausweisen der auf die Daten zugreifenden Organisationseinheit (kein Ausweisen der zugreifenden Person)
    - Ausweisen des Grundes für den Datenzugriff: bspw. durch Angabe durch Rechtsgrundlagen, Prozesse oder Leistungen
    - Die Weitergabe von Personendaten der betroffenen natürlichen Person an eine andere Organisationseinheit
- Explizit vom Umfang von UZ13 ausgeschlossen wurden:
    - Anzeige von Dokumenten, welche mit der natürlichen Person verknüpft sind
    - Erfassung oder Korrektur von Daten durch die betroffene natürliche Person
    - Umsetzung von «Once Only», Förderung des Datenaustausches zwischen Verwaltungsstellen, Förderung zentralisierter Stammdaten, Harmonisierung und Standardisierung von Daten / Prozessen / Schnittstellen / …
    - Erweiterte Nutzungsfreigaben von Daten durch die betroffene natürliche Person
    - Einsicht in die für die betroffene natürliche Person bereitgestellten Nachvollziehbarkeitsinformationen durch Mitarbeitende der öffentlichen Verwaltung
- In die Nachvollziehbarkeitslösung sollen in einem ersten Schritt der Bund, die Kantone, die Gemeinden sowie staatsnahe Organisationen (AHV-Ausgleichskassen, IV-Stellen oder ähnliche) eingebunden werden können

[5] I.e. die natürliche Person kann die entsprechenden Informationen Online (z.B. Website / App) beziehen. Eine grösstenteils analoge Lösung, bei welcher natürliche Personen einer Verwaltungseinheit bspw. einen Brief schreiben müssen, wird in dieser Machbarkeitsstudie nicht berücksichtigt.

4. Bedarf nach Transparenz und Nachvollziehbarkeit

4.1. Schlüsselerkenntnisse

Verschiedene Studien zeigen, dass für **natürliche Personen grundsätzlich** ein **Bedarf** an zusätzlicher **Transparenz** im Umgang der öffentlichen Verwaltung mit ihren **Personendaten** besteht (Abschnitt 4.2). Dabei **variiert** der exakte **Bedarf** und dadurch die geeigneten Massnahmen von Person zu Person. Ein Bedarf von natürlichen Personen nach Nachvollziehbarkeit der Verwendung von Personendaten durch die öffentliche Verwaltung kann erahnt werden, ist aber aktuell nicht durch Fakten erhärtet.

Der «**e-Government Benchmark**» der EU **vergleicht** die **digitalen Angebote** der öffentlichen **Verwaltung** von verschiedenen Ländern (Abschnitt 4.3). Im Bereich der Transparenz im Umgang mit Personendaten besteht für die **Schweiz** verglichen mit anderen Ländern in Europa **Optimierungspotenzial**.

Auch von Seite der **Politik** werden **Forderungen** nach **zusätzlicher Transparenz** und mehr **Nachvollziehbarkeit** im Umgang mit Personendaten gestellt (Abschnitt 4.4). Diese Forderungen sind generell formuliert, ohne dass eine spezifische Lösung vorgeschlagen wird.

4.2. Transparenzbedarf natürlicher Personen im Umgang der öffentlichen Verwaltung mit ihren Personendaten

Ein grundsätzliches Bedürfnis nach zusätzlicher Transparenz bei der Abwicklung von Verwaltungsleistungen wurde beispielsweise in der «Nationalen E-Government-Studie 2019» festgestellt[6]:

> *«Verbesserungspotenzial sehen persönlich interviewte Personen aus der Bevölkerung bei der Unterstützung durch die Behörden, bei der (noch) einfacheren Abwicklung von Online-Dienstleistungen, bei der Transparenz bei der Abwicklung von Online-Dienstleistungen und beim Umfang des Angebotes an Online-Dienstleistungen.»*

Auch der «eGovernment Monitor 2019» der «Initiative 21» stellt einen grossen Transparenzbedarf fest[7]: Die von den Umfrageteilnehmenden am wichtigsten bewerteten Anforderungen an die Umsetzung von «once only» drehen sich um den Datenschutz sowie die persönliche Kontrolle (respektive das Gefühl von Kontrolle) rund um Personendaten. Die als am wichtigsten bewerteten Aussagen sind:

> *«Meine persönlichen Daten sind vollständig geschützt»*
>
> *«Ich kann die Freigabe meiner Informationen jederzeit widerrufen»*
>
> *«Ich habe die vollständige Kontrolle über alle Daten, die über mich gespeichert werden»*
>
> *«Die Handhabung ist einfach und ich kann problemlos zustimmen oder ablehnen, wenn einzelne Behörden meine Daten verwenden wollen»*
>
> *«Ich möchte bei jeder einzelnen Nutzung meiner Daten explizit gefragt werden, ob die Informationen weitergegeben werden dürfen»*

[6] Fokus CH, siehe: https://www.egovernment.ch/de/dokumentation/nationale-e-government-studie-2019/

[7] Fokus DE, AT und CH, siehe: https://initiatived21.de/app/uploads/2019/10/egovernment-monitor-2019.pdf

Diese fünf Anforderungen wurden als wichtiger eingestuft als andere funktionelle Anforderungen wie beispielsweise:

> *«Da die Behörde meine Daten kennt, informiert sie mich aktiv, wenn ich einen Anspruch auf eine bestimmte Leistung habe».*

Auch andere Studien unterstreichen den grundsätzlichen Bedarf nach zusätzlicher Transparenz im Umgang der öffentlichen Verwaltung mit Personendaten. So steht beispielsweise in der Trendstudie Smart Citizen 2020[8]:

> *«Man spürt auch das zunehmende Bedürfnis der Gesellschaft nach Transparenz bei der Datenverwendung und nach der Ausübung der eigenen Entscheidungsmacht.»*

Neben Datenschutz und Datensicherheit[9] besteht folglich mindestens teilweise ein ungedeckter und möglicherweise steigender Bedarf an zusätzlicher Transparenz und Kontrolle im Umgang der öffentlichen Verwaltung mit Personendaten. Mögliche Motive sind exemplarisch in Abbildung 2 aufgeführt. Nicht alle dieser Motive können im Rahmen von UZ13 adressiert werden.

Abbildung 2: Mögliche Anforderungen natürlicher Personen an die Nachvollziehbarkeit von Personendaten durch die öffentliche Verwaltung.

Basierend auf den publizierten Studien lässt sich für natürliche Personen aktuell ein Bedarf nach zusätzlicher Nachvollziehbarkeit im Sinne von UZ13 erahnen – entsprechende Daten fehlen. Es wurden daher im Rahmen dieses Projekts zusätzliche Fragestellungen für die Nationale E-Government-Studie Schweiz 2021 entworfen, um weitere Einsichten zum Bedarf der natürlichen Personen zu erhalten. Die Fragestellungen sind in Anhang A.13 aufgeführt. Die Resultate der Studie werden 2022 publiziert.

[8] Fokus CH, siehe: https://www.ccsmartcitizen.ch/

[9] Siehe auch: https://www2.deloitte.com/ch/de/pages/public-sector/articles/schweizer-misstrauen-e-government-services-wegen-datenschutz-und-datensicherheit.html

4.3. EU-Benchmark zur Transparenz in der öffentlichen Verwaltung

Effiziente und breit akzeptierte digitale Angebote der öffentlichen Verwaltung können im nationalen und internationalen Wettbewerb einen Standortvorteil erzeugen. Die Schaffung von Transparenz im Bereich der Datennutzung ist eine mögliche Massnahme, um das Vertrauen der natürlichen Personen in die digitalen Dienstleistungen der öffentlichen Verwaltung zu stärken und dadurch deren Nutzung zu fördern.

Der «eGovernment Benchmark 2020» der EU[10] vergleicht die digitalen Angebote der öffentlichen Verwaltungen in den verschiedenen Ländern Europas. Unter anderem wird das Thema der Transparenz verglichen. Ein im Benchmark untersuchter Bereich der Transparenz ist die Transparenz der «Personendaten». Es wird untersucht, ob natürliche Personen digitalen Zugang zu ihren persönlichen Daten haben, ob sie inkorrekte Daten melden oder ggf. selbst korrigieren können und ob es dazugehörende Beschwerdeprozesse gibt. Für UZ13 speziell relevant wird auch untersucht, ob natürliche Personen überprüfen können, wer ihre persönlichen Daten verwendet hat (siehe Abbildung 3[11]). Der eGovernment Benchmark der EU berücksichtigt jedoch nicht, ob natürliche Personen die digitalen Angebote der öffentlichen Verwaltung auch nutzen oder ob sie mit diesen zufrieden sind.

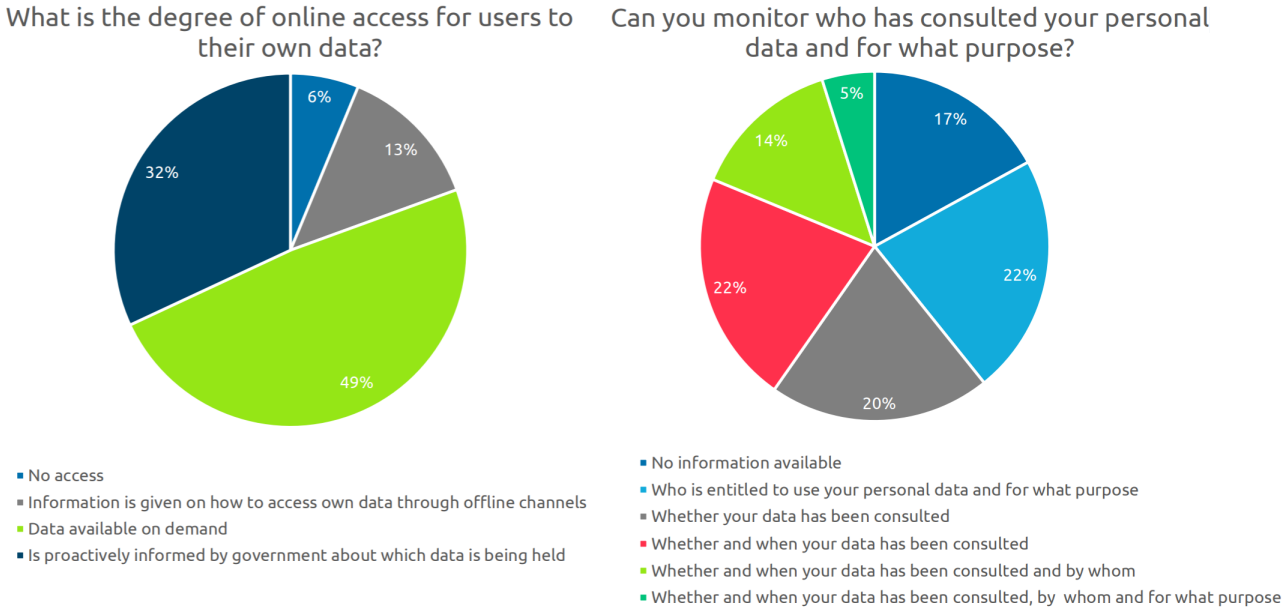

Abbildung 3: Über alle Online-Dienste der EU (EU27+): Können natürliche Personen ihre Daten und deren Nutzung einsehen? (Abbildung 2.14 aus dem eGovernment Benchmark 2021)

[10] Siehe: https://digital-strategy.ec.europa.eu/en/library/egovernment-benchmark-2020-egovernment-works-people

[11] Abbildung aus dem EU eGovernment Benchmark 2021: https://digital-strategy.ec.europa.eu/en/library/egovernment-benchmark-2021 (Creative Commons 4.0, Attribution and Changes)

Die Schweiz hat im Vergleich mit verschiedenen EU-Ländern im Bereich «Transparenz der Nutzung von Personendaten» einen gewissen Nachholbedarf, wie die vergleichsweise schlechte Bewertung der Schweiz in Abbildung 4 zeigt[12]:

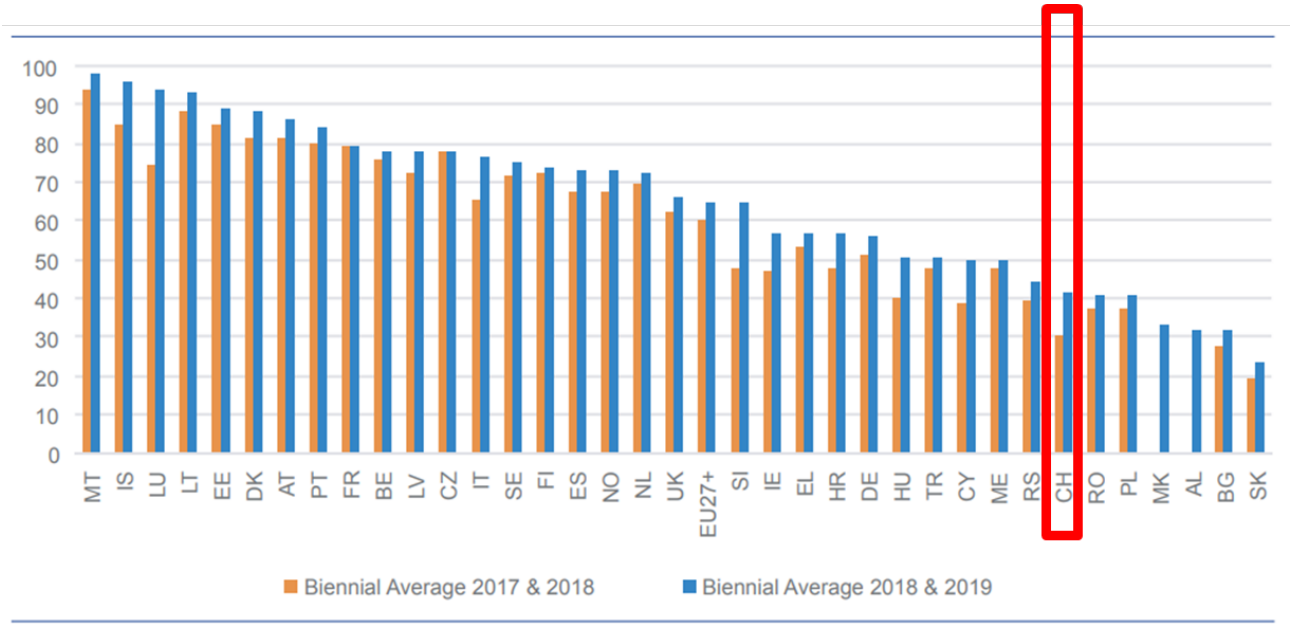

Figure 3.18 Biennial averages for the Transparency of Personal Data indicator per country

Abbildung 4: Die Schweiz schneidet im Vergleich mit den meisten anderen EU-Ländern im Bereich «Transparenz der Personendaten» schlecht ab (rote Box nachträglich hinzugefügt).

Es besteht folglich auch auf Seite der öffentlichen Verwaltung ein Interesse, zusätzliche Transparenz für natürliche Personen zu schaffen.

Auch im Bereich der Digitalisierung des Datenschutzes wurde durch den EU-Benchmark für die Schweiz ein möglicher Handlungsbedarf erkannt: Eine natürliche Person kann per «Auskunftsbegehren gemäss Datenschutzgesetz» Einsicht in die persönlichen Daten erhalten. Dieser Prozess wird von der öffentlichen Verwaltung heute grösstenteils analog in Form von Briefen abgewickelt (siehe auch Abschnitt 5.2).

[12] Abbildung aus dem EU eGovernment Benchmark 2020 entnommen: https://digital-strategy.ec.europa.eu/en/library/egovernment-benchmark-2020-egovernment-works-people
(Creative Commons 4.0, Attribution and Changes)
Die Werte haben sich auch im EU eGovernment Benchmark 2021 nicht signifikant verändert
(siehe «8. Indicator Graphs» hier: https://ec.europa.eu/newsroom/dae/redirection/document/80571)

4.4. Forderungen der Politik nach mehr Transparenz und Nachvollziehbarkeit

Das Thema «Transparenz» ist im Bereich von E-Government bereits heute breit verankert, wie die folgenden Beispiele zeigen. Punktuell wird auch das Thema der Nachvollziehbarkeit der Verwendung von Personendaten durch die öffentliche Verwaltung thematisiert.

E-Government Strategie Schweiz 2020-2023 sowie daraus abgeleitete kantonale Strategien

Das Umsetzungsziel 13 ist ein Umsetzungsprojekt der E-Government Strategie Schweiz 2020-2023[13] und unterstützt das Ziel:

«Wissen zur Digitalisierung der Verwaltung fördern und Vertrauen stärken»

Die von den Kantonsregierungen unterzeichnete «öffentlich-rechtliche Rahmenvereinbarung über die E-Government Zusammenarbeit in der Schweiz 2020»[14] stützt sich auf die E-Government Strategie Schweiz. Die Kantone tragen folglich die Ziele des Bundes im Bereich E-Government mit. Die meisten Kantone haben die Ziele der E-Government Strategie Schweiz in ihren eigenen Strategien nachgeführt[15].

Tallinn Declaration on eGovernment

Die «Tallinn Declaration on eGovernment» stellt europaweit eine gemeinsame Basis für die Weiterentwicklung von digitalen Verwaltungsdienstleistungen dar. Die Tallinn Declaration wurde auch von der Schweiz unterzeichnet[16]. Die Grundsätze der Tallinn Declaration lassen sich auch in der E-Government Strategie der Schweiz 2020-2023 wieder auffinden. Es wurden fünf Prinzipien definiert, wovon eines für UZ13 relevant ist:

«Openness and transparency»

Dieses Prinzip besagt, dass natürliche und juristische Personen ihre Daten einfacher verwalten können sollen. Dabei inbegriffen sind der Zugriff auf die Daten, die Korrektur von Daten, die Erteilung und der Entzug von Berechtigung zur Verwendung der Daten und auch die Einsicht in die Verwendung der Daten[17]. Die Tallinn Declaration wurde durch die «Berlin Declaration on Digital Society and Value-based Digital Government» ergänzt[18], welche jedoch bisher von der Schweiz nicht unterzeichnet wurde.

Leitlinien der Kantone zur Digitalen Verwaltung

Die Konferenz der Kantonsregierungen hat Leitlinien für die digitale Verwaltung erarbeitet[19]. In diesen Leitlinien werden sowohl übergeordnete Ziele und Prinzipien als auch Handlungsfelder und Handlungsansätze definiert. So ist beispielsweise definiert:

«Transparenz der Datennutzung: Das Wissen innerhalb der Verwaltung ist zu erhöhen. Es bedarf klarer Angaben bzw. einer Offenlegung, wer für welche Zwecke die Daten wo abspeichert und wie nutzt (z.B. Logbook in Estland).»

---

[13] Die Medienmitteilung ist unter folgendem Link einsehbar: https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-72924.html
Die E-Government Strategie Schweiz 2020–2023 ist unter folgendem Link einsehbar: https://www.egovernment.ch/files/7315/9406/6023/E-Government-Strategie-Schweiz-2020-2023_D_def.pdf

[14] Siehe: https://www.egovernment.ch/de/umsetzung/offentlich-rechtliche-rahmenvereinbarung-uber-die-e-governme/

[15] Details siehe E-Government Schweiz Jahresbericht 2019: https://www.egovernment.ch/files/9615/8885/8087/E-Gov-CH-Jahresbericht-2019_web.pdf

[16] Siehe: https://www.isb.admin.ch/isb/de/home/dokumentation/medienmitteilungen/newslist.msg-id-68342.html

[17] «For the principle of openness and transparency, we will make it possible for citizens and businesses to better manage (e.g. access, check and inquire about the use of, submit corrections to, authorise (re)use of) their personal data held by public administrations, at least in base registries and/or similar databases where feasible;»

[18] Siehe: https://digital-strategy.ec.europa.eu/en/news/berlin-declaration-digital-society-and-value-based-digital-government

[19] https://kdk.ch/uploads/media/Leitlinien-E-Government_20180927.pdf

Diskussionspapier Netzwerk Digitale Selbstbestimmung

Das «Netzwerk Digitale Selbstbestimmung» bestehend aus Vertretern der Bundesverwaltung, der Forschung und der Wirtschaft hat 2020 ein Diskussionspapier verfasst[20], in welchem diskutiert wird, wie natürliche Personen ihr «digitales Ich» besser selbstbestimmt leben können. Es wurden vier Prinzipien definiert, wovon zwei für UZ13 relevant sind, jedoch über den Umfang von UZ13 hinausgehen:

«Transparenz und Vertrauen»

«Kontrolle und selbstbestimmte Weitergabe»

[20] https://digitale-selbstbestimmung.swiss/home/

5. Situationsanalyse

5.1. Schlüsselerkenntnisse

Als Startpunkt der Situationsanalyse wurde eine Übersicht bezüglich der Möglichkeiten erstellt, welche eine natürliche Person bereits heute besitzt, um Einsicht in die von der Verwaltung gespeicherten eigenen Personendaten zu erhalten (Abschnitt 5.2). Gemäss Datenschutzgesetz darf **jede Person** von grundsätzlich jeder Verwaltungseinheit **per Brief verlangen**, **Einsicht** in die von der jeweiligen Verwaltungseinheit gespeicherten **eigenen Personendaten** zu bekommen. Begründete Ausnahmen bestehen beispielsweise im Bereich von laufenden Strafverfahren. Die angeschriebene Verwaltungseinheit muss verantwortlich für die entsprechende Datensammlung sein und hat **innerhalb** von **30 Tagen** wiederum **schriftlich** eine **Antwort** zu senden.

Dieses heutige **Verfahren** zur Auskunftserlangung über die eigenen Personendaten ist für natürliche Personen **aufwändig** und **kompliziert**. Es **skaliert** auch auf **Verwaltungsseite nicht**, wenn viele natürlichen Personen ein Auskunftsbegehren stellen.

Um eine neue Nachvollziehbarkeitslösung für die Personendaten von natürlichen Personen bereitzustellen, ist als erstes ein Verständnis darüber notwendig, wie die entsprechenden Personendaten auf den Systemen der öffentlichen Verwaltung erfasst werden. Die **Daten** werden von Verwaltungseinheiten im Allgemeinen **im Rahmen** von **Prozessen erfasst/bearbeitet**, **welche** wiederum aus verschiedenen **Verwaltungsleistungen bestehen** (Abschnitt 5.3).

Die **Grundlage** für diese **Prozesse** und **Leistungen** sind **Gesetze** und **Verordnungen** («Legalitätsprinzip»). In der Theorie wäre daher durch das Studium der entsprechenden Rechtstexte ein grosses Mass an Transparenz über die Bearbeitung von Personendaten gegeben – in der Praxis ist das Studium der Gesetztestexte für natürliche Personen jedoch zu komplex und aufwändig. Es kommt erschwerend dazu, dass **Verwaltungsprozesse über** mehrere **Organisationseinheiten**, **Fachbereiche** oder sogar über die drei **Staatsebenen hinweg** stattfinden können sowie eine Vielzahl von verschiedenen IT-Systemen involviert sein können.

Je «**kundenfreundlicher**» der **Verwaltungsprozess** gestaltet wird – i.e. je mehr die Verwaltung den Prozess ohne Zutun der natürlichen Person orchestriert – **desto weniger transparent** wird dieser Prozess und dadurch die Datenverarbeitung für die betroffene **natürliche Person**. Für die natürliche Person spielt auch der Kontext der Datenverarbeitung eine wichtige Rolle, wie folgende Beispiele zeigen: Bei der Einreichung der Steuererklärung ist es offensichtlich, dass Steuerdaten erfasst werden. Bei der Beantragung der Prämienverbilligung werden oftmals ebenfalls im Hintergrund Steuerdaten zwischen Verwaltungseinheiten ausgetauscht, ohne dass dies für die natürliche Person ersichtlich wäre.

Die nächste Herausforderung sowohl für die Erstellung einer Nachvollziehbarkeitslösung als auch für die natürliche Person, welche eine Übersicht über die Verwendung der Personendaten haben möchte, ist die **grosse Anzahl** von **Datensammlungen** und **IT-Systemen** der Schweizer Verwaltung in welchen **Personendaten verarbeitet** werden (Abschnitt 5.4). Eine **grobe Abschätzung** geht von einer **vierstelligen Anzahl** von **IT-Systemen** der **öffentlichen Verwaltung** aus, in welchen Daten über natürlichen Personen gespeichert und verarbeitet werden. Es wird zudem eine **fünfstellige Anzahl** von **Datensammlungen** geschätzt, welche Personendaten enthalten.

Eine grobe Analyse dieser grossen Anzahl an Datensammlungen und Systemen führt zu folgenden Erkenntnissen:

- Nicht alle Systeme sind gleich relevant (Wichtigkeit der Daten, Menge der Datensätze, Sensitivität der Daten, …)
- Der Standardisierungsgrad der Systeme variiert stark (Abschnitt 5.5.1).

- Es gibt weiterhin Datensammlungen, welche nicht mittels eines dedizierten IT-Systems gepflegt werden (bspw. auf Papier, mit Excel, Falldossiers in Word, …)
- Es gibt Systeme, auf welche eine Vielzahl von berechtigten Stellen zugreifen dürfen.

Neben den IT-Systemen der Verwaltung, auf welchen die Daten der natürlichen Personen erfasst und bearbeitet werden, gibt es auch diverse **Plattformen** zum **Datenaustausch** (Abschnitt 5.5.3). Die Anbindung solcher Plattformen zum Datenaustausch an die Nachvollziehbarkeitslösung würde es erlauben, den Austausch von Personendaten zwischen verschiedensten Systemen für natürliche Personen sichtbar zu machen. Die in der föderalen Verwaltung für den sicheren Datenaustausch am meisten eingesetzte Plattform ist «sedex». sedex ist Ende-zu-Ende verschlüsselt, was bedeutet, dass lediglich der Sender und der Empfänger der Nachricht deren Inhalt kennen. Die Nachvollziehbarkeitslösung könnte somit **mittels sedex keine Auskunft** über den **Inhalt** der zwischen den Verwaltungseinheiten **ausgetauschten Daten** erhalten.

Im Bereich des E-Government Ökosystems **fehlen** in der **Schweiz** aktuell verschiedene **wichtige** «**Enabler**» (Abschnitt 5.5.2). Dies sind unter anderem eine **national anerkannte E-ID**, ein **verwaltungsweit** einheitliches **Datenmanagement**, die breite Verwendung **einheitlicher** und **eindeutiger Identifikatoren** für natürliche Personen sowie ein fehlendes **nationales E-Government Portal** für **natürliche Personen**. Diese Themen werden aktuell mit verschiedenen Vorhaben adressiert, sodass sich die Ausgangslage in den nächsten Jahren weiterentwickeln wird. Das Fehlen dieser «Enabler» verhindert die Umsetzung einer skalierbaren Nachvollziehbarkeitslösung nicht a priori, erschwert jedoch deren allfällige Umsetzung.

Als **Inspiration** werden als nächstes Nachvollziehbarkeitslösungen aus anderen Ländern vorgestellt (Abschnitt 5.6.1). **Estland** und **Luxemburg** haben bereits **funktionierende Nachvollziehbarkeitslösungen** und in **Dänemark** befindet sich die Nachvollziehbarkeitslösung im **Aufbau**. In allen drei Ländern ist die Nachvollziehbarkeitslösung ein **Teil** von **zentral angebotenen E-Government Services** für natürliche Personen. Ebenfalls gemeinsam an allen Lösungen ist, dass die Nachvollziehbarkeitslösung **lediglich** für **ausgewählte Systeme** / Datensammlungen **angeboten** wird.

Das Ende 2020 eingeführte **elektronische Patientendossier** der Schweiz **setzt** gewisse Aspekte einer **Nachvollziehbarkeitslösung** für ein **spezifisches System um** (Abschnitt 5.6.2). Die Erfahrungen der nächsten Phase, in welcher die Verwendung des Patientendossiers ausgedehnt wird, können für eine Nachvollziehbarkeitslösung genutzt werden.

5.2. Aktuelle Auskunftsmöglichkeiten für natürliche Personen im Bereich Personendaten

Basierend auf dem Auskunftsrecht[21] (Datenschutzgesetz (DSG) Artikel 8 und 9 – neues DSG Art. 20, 21) kann jede Person vom Inhaber einer Datensammlung Auskunft darüber verlangen, ob Daten über sie bearbeitet werden, zu welchem Zweck die Daten bearbeitet werden sowie basierend auf welcher Rechtsgrundlage die Daten bearbeitet werden. Mit dem Auskunftsrecht besteht bereits heute für natürliche Personen die Möglichkeit, ein gewisses Mass an Transparenz über den Umgang der öffentlichen Verwaltung mit ihren Personendaten zu erlangen.

Auf Seiten der antragstellenden natürlichen Person sieht der Auskunftsprozess gemäss gesetzlicher Minimalvorgabe aktuell wie folgt aus:

1. Die natürliche Person muss die für eine Auskunft, respektive für das relevante System, zuständige Verwaltungseinheit (bspw. Amt) identifizieren.
2. Die natürliche Person muss anschliessend die Kontaktinformationen der zuständigen Verwaltungseinheit in Erfahrung bringen.
3. Als nächstes muss ein Brief in Papierform an die zuständige Verwaltungseinheit geschickt werden. Sind Auskünfte von mehreren Verwaltungseinheiten gewünscht, ist an jede Verwaltungseinheit ein separates Schreiben zu senden. Für Identifikationszwecke ist dem Schreiben die Kopie eines amtlichen Dokumentes (Pass oder Identitätskarte) beizulegen.
4. Die angeschriebene Verwaltungseinheit hat anschliessend 30 Tage Zeit, um eine schriftliche Antwort zu senden.

Der Aufwand für eine natürliche Person ist mit dem heutigen System hoch, um eine Auskunft über die Verwendung der persönlichen Daten durch die öffentliche Verwaltung zu erhalten, insbesondere wenn mehrere Verwaltungseinheiten involviert sind.

Da die Anfragen bei der zuständigen Verwaltungseinheit in schriftlicher Form eintreffen und ebenso beantwortet werden müssen, ist davon auszugehen, dass bei einer Anfrage gemäss Datenschutzgesetz auch auf Verwaltungsseite ein substanzieller Aufwand entsteht.

Die von den Kantonen angebotenen Hilfestellungen an natürliche Personen variieren stark. Es wurden drei Kategorien von Hilfestellungen identifiziert:

- Beschreibung der Rechte von natürlichen Personen sowie der Prozesse, über welche diese Rechte ausgeübt werden können.
- Bereitstellung von Musterbriefen für Auskunftsbegehren gemäss Datenschutzgesetz.
- Die Bereitstellung von einem öffentlich einsehbaren Register der Datensammlungen.

Eine Übersicht darüber, welcher Kanton welche Hilfestellungen anbietet, ist in Anhang A.3 aufgeführt. Etwa zwei Drittel der Kantone verfügen über ein zentrales und öffentlich zugängliches Register der vorhandenen Sammlungen von Personendaten.

Die heutige Situation erlaubt es einer natürlichen Person kaum, sich mit vertretbarem Aufwand eine umfassende Übersicht zu verschaffen, welche Verwaltungseinheiten in welchen Datensammlungen oder Systemen potenziell Daten über sie gespeichert haben und entsprechend ihr Recht auf Auskunft auszuüben. Den Autoren dieser Machbarkeitsstudie ist kein Kanton bekannt, der seinen Kunden einen digitalisierten Prozess zum Auskunftsrecht anbietet.

[21] Siehe Datenschutzgesetz SR 235.1, Art. 8

Diverse Kantone haben E-Government Plattformen aufgebaut, bei welchen natürliche Personen bei Bedarf ausgewählte Interaktionen mit der Verwaltung digital durchführen können (für Details siehe Anhang A.4). Punktuell ist auch eine Einsicht in erfasste Daten möglich. Es betreiben jedoch nicht alle Kantone eigene E-Government Plattformen und auch die Einsichtsmöglichkeiten in erfasste Daten sind im Allgemeinen stark beschränkt. Die heute bestehenden E-Government-Plattformen bieten zwar vielfältige Dienstleistungen für natürliche Personen, sind aber im Allgemeinen keine signifikante Hilfe dabei, Transparenz über die Verwendung der Personendaten zu erhalten.

5.3. Verwaltungsprozesse zur Verarbeitung von Personendaten

Natürliche Personen interagieren mit der öffentlichen Verwaltung üblicherweise im Rahmen von Geschäftsfällen: Entweder benötigt die natürliche Person eine Dienstleistung von der öffentlichen Verwaltung und stösst somit einen Prozess an oder die öffentliche Verwaltung kontaktiert die natürliche Person aufgrund von einem bereits vorgängig angestossenen Prozess. Im Rahmen dieser Prozesse findet der Personendatenaustausch zwischen den natürlichen Personen und der Verwaltung statt. Beispiele für solche Prozesse sind der Umzug einer natürlichen Person an einen neuen Wohnort (Prozess wird durch die natürliche Person selbst angestossen) oder die Erhebung von Steuern (der Prozess wird üblicherweise von der öffentlichen Verwaltung angestossen).

Die öffentliche Verwaltung erfasst und speichert die Personendaten basierend auf den rechtlichen Grundlagen und soweit zur Aufgabenerfüllung notwendig («Datensparsamkeit»). Zudem tauscht die öffentliche Verwaltung im Rahmen der Prozesse oftmals auch intern oder mit Dritten Personendaten aus, sofern dies wiederum durch rechtliche Grundlagen geregelt ist und für die Aufgabenerfüllung notwendig ist.

Sämtliche Aktionen der öffentlichen Verwaltung basieren gemäss Legalitätsprinzip (Verfassung) auf rechtlichen Grundlagen (Gesetze, Verordnungen, …). In der Theorie ist die öffentliche Verwaltung daher grösstenteils transparent. In der Praxis stellen die umfangreichen und komplexen rechtlichen Grundlagen für natürliche Personen im Allgemeinen keine wirkliche Hilfe dar, basierend auf welcher die Verwendung von Personendaten durch die öffentliche Verwaltung besser verstanden werden könnte.

5.3.1. Prozesse über mehrere Verwaltungseinheiten und Staatsebenen

Für die erfolgreiche Abwicklung eines Prozesses werden teilweise innerhalb einer Staatsebene mehrere Verwaltungseinheiten, resp. sogar Verwaltungseinheiten mehrerer Staatsebenen involviert. Gemäss eCH-0126 («Rahmenkonzept Vernetzte Verwaltung Schweiz») besteht in diesem Fall ein Prozess aus verschiedenen Leistungen[22].

Sobald die verschiedenen Prozessschritte (Leistungen) durch die Verwaltung selbst angestossen und abgewickelt werden, ist es für die natürliche Person schwer nachzuvollziehen, welche Verwaltungseinheit wann welche Daten wieso erhält, nutzt, verändert und wiederum weitergibt, sowie welche Stellen auf diese Daten zugreifen. Weitere Details sind in Anhang A.5 aufgeführt.
Zur Gewinnung einer Übersicht über Themengebiete, welche für natürliche Personen relevant sein können, wurden eCH-0049/Beilage1 und eCH-0145 herangezogen und in

[22] eCH-0126 siehe: https://www.ech.ch/de/dokument/fa1c7c13-60bc-4ca5-8b81-ee66f689c0d1

Tabelle 2 festgehalten[23]. Für jedes der aufgeführten Themengebiete wurde von den Autoren der Machbarkeitsstudie eine indikative Abschätzung gemacht, wie oft eine durchschnittliche natürliche Person direkten oder indirekten Kontakt (bspw. via Arbeitgeber) mit der öffentlichen Verwaltung hat[24]. Es ist davon auszugehen, dass bei einer Vielzahl dieser Interaktionen zwischen natürlichen Personen und der Verwaltung[25] Daten erfasst, genutzt, aufbewahrt und ausgetauscht werden.

[23] Die Tabelle dient lediglich als Illustration und stellt keinen Anspruch an die Vollständigkeit.

[24] Für gewisse Prozess-Themengebiete gibt es relativ genaue Statistikdaten, für andere musste eine grobe Schätzung gemacht werden. Die genannten Kategorien (regelmässig, oft, manchmal, selten) sollen einen Anhaltspunkt für die Häufigkeit geben, ohne dass diese explizit quantifiziert wird.

[25] Im Sinne der Grobanalyse werden die Themen der Sozialversicherungen ebenfalls aufgeführt.

Tabelle 2: Gründe für Kontakt zwischen nat. Personen und der öffentlichen Verwaltung (inkl. weiterer Sozialversicherungen)

Grund für Kontakt mit der öffentlichen Verwaltung	geschätzte Häufigkeit der Interaktion
Steuern (Bund / Kanton / Gemeine / Kirche)	regelmässig
Einzahlung AHV (meist via Arbeitgeber)	regelmässig
Ausübung der politischen Rechte (Abstimmen, Wählen, …)	regelmässig
Familienzulagen (meist via Arbeitgeber)	oft
Vergünstigungen (Krankenkasse, KITA, ...)	oft
Bezug / Beglaubigung Dokumente (Bestätigung für FamilienGA, Betreibungsregister, Strafregister, ...)	oft
Wareneinfuhr (Zoll)	oft
Motorfahrzeugkontrolle (StVA)	oft
Umzug	oft
Bezug Altersrente (AHV)	oft
Militärdienst / Zivilschutz / Zivildienst / (freiwillige) Feuerwehr	oft
Bussen	oft
Bezug Ausweisdokumente (Pass, ID, Führerausweis, ...)	oft
Besuch obligatorische / überobligatorische Schule	oft
Altenpflege	manchmal
Haustiere (Hundesteuer, bewilligungspflichtige Tiere, ...)	manchmal
Tod eines nahen Angehörigen	manchmal
Strafverfolgung / Strafvollzug	manchmal
Sozialhilfe / Nothilfe	manchmal
Konsularische Dienstleistungen	selten
Krankheit / Invalidität (AHV / IV)	selten
Immigration	selten
Arbeitslosigkeit (ALV)	selten
Vormundschaft	selten
Geburt / Adoption eines Kindes	selten
Heirat / eingetragene Partnerschaft	selten
Stipendien	selten
Betreibung	selten
Erwerb von (Wohn)Eigentum	selten
Einbürgerung	selten
Waffenerwerb	selten
Baugesuch	selten
Asylverfahren	selten
«Zulassungen» (Fischereipatente, …)	selten

5.3.2. *Beispiel: Prozesse im Bereich «Personenmeldewesen»*

Wie in Abschnitt 5.3.1 aufgeführt, kann die Abwicklung eines Prozesses verschiedene Verwaltungseinheiten und Staatsebenen betreffen und entsprechend komplex sein. Abbildung 5 zeigt am Beispiel von Prozessen[26] aus dem Bereich «Personenmeldewesen»[27] die grosse Anzahl beteiligter IT-Systeme und Schnittstellen dar.

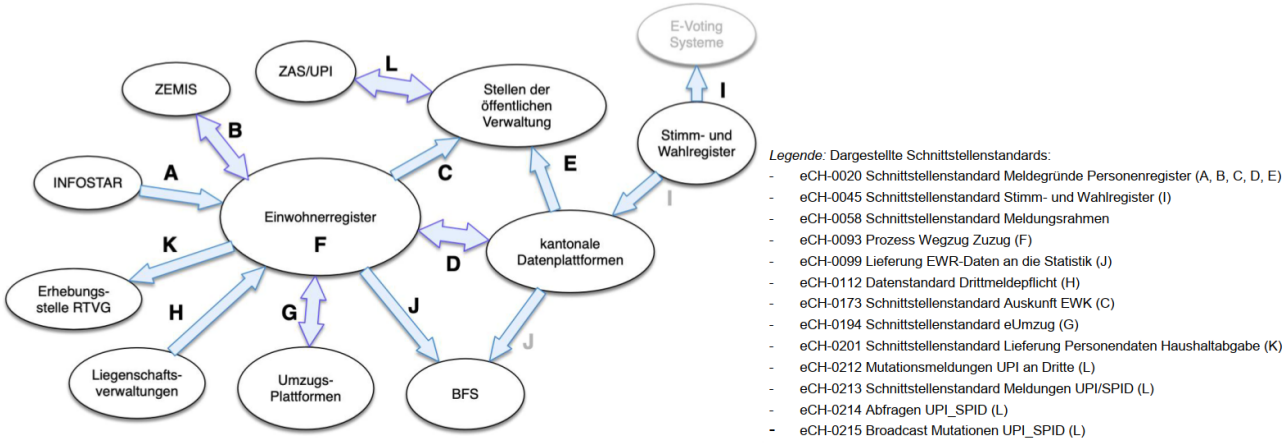

Abbildung 5: Darstellung der Datenflüsse und der verwendeten Schnittstellen im Personenmeldewesen[28]

5.3.3. *Der Kontext der Datenverwendung*

Wird im Rahmen einer Nachvollziehbarkeitslösung einer natürlichen Person ein Datenzugriff angezeigt, so ist der Kontext dieses Zugriffs relevant. Folgende Beispiele zeigen dies exemplarisch:

- Der Zugriff auf die Steuer- und Adressdaten durch die kantonale Steuerbehörde im Rahmen der Bearbeitung einer gerade eingereichten Steuererklärung dürfte im Allgemeinen nicht weiter überraschen.
- Der Zugriff auf die gleichen Daten durch die kantonale Steuerbehörde nach abgeschlossener Bearbeitung der Steuererklärung und Bezahlung der Steuerrechnung könnte die betroffene natürliche Person überraschen.
- Der Zugriff auf die gleichen Daten durch die für die Prämienverbilligung zuständige Stelle (in vielen Kantonen wird der Anspruch für die Prämienverbilligung auf Basis des steuerbaren Einkommens und Vermögens berechnet) könnte die betroffene natürliche Person ebenfalls überraschen.
- Der Zugriff auf die gleichen Daten durch kantonale Strafverfolgungsbehörden wird die natürliche Person mit grosser Sicherheit überraschen. Falls dieser Zugriff beispielsweise im

[26] In der Abbildung wird von Geschäftsfällen gesprochen. Im Rahmen dieser Studie wird von Prozessen gesprochen (basierend auf den eCH Standards), was mit Geschäftsfällen gleichzusetzen ist.

[27] Als Beispiel für einen solchen Geschäftsfall kann ein Umzug einer natürlichen Person dienen: Die Person meldet sich in einer Gemeinde ab und in einer anderen Gemeinde mit Namen und neuer Adresse wieder an.

[28] Abbildung aus der Studie «Strategie Datenmanagement und Data-Governance « des Kantons Zürich: https://www.zh.ch/content/dam/zhweb/bilder-dokumente/organisation/staatskanzlei/digitale-verwaltung-und-e-government/studiep_projekt_datenmanagement_data-governance
In der Grafik zu beachten: Diverse der Kreise entsprechen nicht einer Organisationseinheit / einem System sondern symbolisieren eine Sammlung von Organisationseinheiten / Systemen.

Rahmen eines laufenden Strafverfolgungsverfahren stattfindet[29], dürfte dieser Zugriff durch die Nachvollziehbarkeitslösung der natürlichen Person nicht mitgeteilt werden.

Wie obige Beispiele zeigen, spielt der Kontext der Datenverwendung für die natürliche Person eine wichtige Rolle.

5.3.4. Rollen-Sicht

Ergänzend zur Prozess-Sicht ist es möglich, die Interaktion zwischen natürlichen Personen und der öffentlichen Verwaltung auch aus der Sicht der jeweiligen Rolle zu charakterisieren, welche eine natürliche Person bei der Interaktion einnimmt. Folgende Liste zeigt Beispiele für mögliche Rollen für Interaktionen mit Verwaltungseinheiten (nicht abschliessend):

- Steuerzahler oder Steuerzahlerin
- Soldat oder Soldatin
- Bezüger oder Bezügerin von Sozialleistungen
- Fahrer oder Fahrerin eines Motorfahrzeugs

5.4. Mengengerüst und Systeme: Personendatensammlungen der schweizerischen Verwaltungseinheiten

Für die Umsetzung der Nachvollziehbarkeitslösung müssen ausgewählte oder sogar alle IT-Systeme sowie die darauf gespeicherten Datensammlungen[30], auf welchen die schweizerischen Verwaltungen der verschiedenen Staatsebenen Personendaten verarbeiten, an diese Lösung angeschlossen werden[31]. Wie dieser Abschnitt aufzeigt, würde eine Auflistung sämtlicher IT-Systeme, auf welchen Personendaten verarbeitet werden, den Rahmen dieser Machbarkeitsstudie sprengen. Es wird daher eine aggregierte Abschätzung der Anzahl der betroffenen IT-Systeme gemacht (5.4.1, 5.4.2, 5.4.3). Abschnitt 5.4.4 macht einen Versuch, das erarbeitete Mengengerüst einzuordnen. Abschnitt 5.4.5 zeigt exemplarisch eine Auswahl von Systemen in welchen Personendaten bearbeitet werden. Abschnitt 5.4.6 zeigt exemplarisch anhand des ZEMIS-Systems, wie der Datenaustausch zwischen verschiedenen Verwaltungseinheiten geregelt ist. Für die Umsetzung der Nachvollziehbarkeitslösung ist nicht nur die reine Anzahl von separat betriebenen IT-Systemen relevant, sondern auch, ob diese standardisiert und ob die Daten harmonisiert sind (Abschnitt 5.5.1).

[29] Zu klären wäre hier allenfalls, ob beispielsweise nach Abschluss eines Verfahrens ein Recht der natürlichen Person darauf besteht, die entsprechenden Datenzugriffe zu sehen.

[30] Auf dem gleichen IT-System oder verschiedenen Instanzen davon können mehrere verschiedene Datensammlungen gespeichert sein.

[31] Es sind verschiedenste Lösungsansätze denkbar: eine zentralisierte Lösung, kantonale Lösungen, … Der Begriff «Nachvollziehbarkeitslösung» wird im Sinne des Gesamtsystems verwendet, welches auch aus verschiedenen Teilsystemen bestehen kann.

5.4.1. *Mengengerüst der Datensammlungen und Systeme zur Verarbeitung von Personendaten des Bundes*

Eine relativ einfache Methode um eine grobe Abschätzung der Anzahl von Datensammlungen auf Bundesebene zu erhalten, liefert die Umsetzung einer Forderung des Datenschutzgesetzes: Gemäss Artikel 11a des aktuell gültigen Datenschutzgesetztes der Schweiz[32] müssen sämtliche Bundesbehörden ihre Datensammlungen mit Personendaten anmelden (Ausnahmen bestehen gemäss Artikel 11a des Datenschutzgesetzes und Artikel 4 der Verordnung zum Datenschutzgesetz[33]). Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) führt ein öffentlich einsehbares Register, in welchem diese Datensammlungen aufgeführt sind[34].

Stand 2020 sind in diesem Register über 1000 Datensammlungen von Bundesorganen eingetragen. Zu jeder Datensammlung sind folgende Informationen vorhanden:

- Bezeichnung und Zweck der Datensammlung
- Adresse des Inhabers der Datensammlung
- Rechtsgrundlagen für die Datensammlung
- Auflistung sämtlicher Kategorien von Personendaten, welche in der Datensammlung enthalten sind

Eine stichprobenartige Durchsicht der gemeldeten Datensammlungen lässt vermuten, dass die über 1000 gemeldeten Datensammlungen grösstenteils in spezifischen Fachanwendungen gepflegt werden. Es ist davon auszugehen, dass der Standardisierungsgrad bei den Fachanwendungen auf Bundesebene klein ist. Als Konsequenz muss jede Anwendung separat an eine allfällige Nachvollziehbarkeitslösung angebunden werden, was einen entsprechend grossen Aufwand erzeugt. Auch die gespeicherten Daten dürften in vielen Fällen weder standardisiert noch harmonisiert sein[35].

5.4.2. *Mengengerüst der Datensammlungen und Systeme zur Verarbeitung von Personendaten der Kantone*

Analog zur Bundesebene verfügen auch die Kantone über eigene Gesetze, welche den Umgang mit Personendaten regeln[36]. Folgende Liste zeigt exemplarisch eine Übersicht über Datensammlungen mit Personendaten in zufällig ausgewählten verschiedenen grösseren und kleineren Kantonen (Stand 2020):

- Kanton Bern[37]: Es werden ca. 500 Applikationen gelistet. Es handelt sich dabei grösstenteils um unterschiedliche Fachanwendungen.
- Kanton Thurgau[38]: Es werden ca. 180 Ämter und Stellen gemeldet.
- Kanton Uri[39]: Es werden 140+ Datensammlungen aufgeführt.

---

[32] Stand 1. März 2019, siehe https://www.fedlex.admin.ch/eli/cc/1993/1945_1945_1945/de
Die Überarbeitung des Datenschutzgesetzes ist an dieser Stelle nicht relevant, da das Register basierend auf der «alten» Version aufgebaut wurde.

[33] https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/handel-und-wirtschaft/unternehmen/anmeldung-einer-datensammlung.html

[34] https://www.datareg.admin.ch/

[35] Es gibt in einigen Bereichen Bestrebungen, die Datensammlungen zu standardisieren und harmonisieren – vgl. bspw. https://www.bfs.admin.ch/bfs/de/home/register/personenregister/registerharmonisierung.html
oder auch https://www.bfs.admin.ch/bfs/de/home/nadb/nadb.html

[36] Siehe auch: https://www.edoeb.admin.ch/edoeb/de/home/dokumentation/datenschutz/schweiz.html

[37] http://registerdatensammlungen-be.instanthost.ch/

[38] https://www.datenschutz-tg.ch/re/

- Kanton Appenzell Ausserrhoden[40]: Es werden 200+ Datensammlungen aufgeführt.
- Kanton Waadt[41]: Es werden 330+ Datensammlungen aufgeführt.

Während gewisse IT-Systeme auf Kantonsebene standardisiert sind (beispielsweise im Bereich der Arbeitslosenversicherung[42]), ist eine Vielzahl spezifisch für den jeweiligen Kanton und die jeweilige Anwendung entwickelt worden. Eine Standardisierung über die Kantone hinweg ist aufgrund von unterschiedlichen rechtlichen Grundlagen nicht immer einfach möglich. Die Konferenz der Kantonsregierungen (KDK) hat die mangelnde Standardisierung als Problem erkannt und mit den «Leitlinien der Kantone zur Digitalen Verwaltung»[43] zusätzliche Schritte in Richtung Standardisierung beschlossen.

Der Kanton Appenzell Ausserrhoden stellt im Register der Datensammlungen bei diversen Datensammlungen die Information zur Verfügung, in welchem IT-System diese gepflegt werden. Anhand dieses Beispiels kann eine exemplarische Übersicht über die Standardisierung von IT-Systemen zu Verarbeitung von Personendaten erlangt werden. Eine grobe Analyse ergibt:

- Ca. 10-20% der Datensammlungen sind «manuell» erfasst (Papierablage, Excel Liste, Kartei, Falldossiers, Word-Dateien, …).
- Ca. 10% werden in generischen Datenbanken (Access-Datenbank) erfasst.
- Einzelne IT-Systeme tauchen mehrmals[44] auf, die Mehrheit aber nur einmalig

Basierend auf den gewonnenen Erkenntnissen ergeben sich folgende Schlussfolgerungen:

- Es gibt im Durchschnitt pro Kanton eine Vielzahl (100+) von verschiedenen IT-Applikationen, in welchen die Datensammlungen gepflegt werden. Teilweise werden verschiedene Datensammlungen in den gleichen Applikationen verwaltet (i.e. es gibt weniger Applikationen als Datensammlungen).
- Gewisse Datensammlungen werden heute in einer Art und Weise gepflegt, welche für eine automatisierte Nachvollziehbarkeitslösung nicht geeignet sind (manuell, Excel, Word, Kartei, …).
- Viele Daten werden redundant oder sogar mit unterschiedlicher Aktualität gehalten oder verarbeitet.

5.4.3. Mengengerüst der Datensammlungen und Systeme zur Verarbeitung von Personendaten der Gemeinden

Auch auf Gemeindeebene werden für verschiedene Aufgaben Personendaten gesammelt. Je nach Grösse der Gemeinde variieren die Anforderungen an die IT-Unterstützung und folglich auch die eingesetzte Software. Während die kleinsten Gemeinden der Schweiz lediglich eine zweistellige Einwohnerzahl haben, hat die grösste Gemeinde der Schweiz – die Stadt Zürich – mit ca. 420'000 Einwohnern mehr Einwohner als die Mehrheit der Schweizer Kantone.

Bei kleineren Gemeinden kommt üblicherweise eine Gemeindelösung zum Einsatz. Je nach Anbieter werden in der Gemeindelösung verschiedene Verwaltungsprozesse sowie die Verwaltung von

---

[39] https://www.ur.ch/publikationen/7680

[40] https://www.ar.ch/verwaltung/datenschutz-kontrollorgan/register-der-datensammlungen/

[41] https://prestations.vd.ch/pub/101049/search/advanced

[42] Siehe: https://www.fedlex.admin.ch/eli/cc/2016/675/de#a3

[43] Siehe: https://kdk.ch/uploads/media/Leitlinien-E-Government_20180927.pdf

[44] beispielsweise die «Archivdatenbank» (9 mal), Axioma (6 mal) oder scopeArchiv (19 mal)

beispielsweise Einwohnerdaten unterstützt[45]. Die Anzahl an Anbietern[46] solcher Gemeindelösungen ist klein[47]. Der Markt ist jedoch aktuell im Umbruch[48], sodass davon auszugehen ist, dass sich in den nächsten Jahren noch weitere Verschiebungen ergeben könnten.

Es ist davon auszugehen, dass insbesondere bei kleineren Gemeinden gewisse Aufgaben mittels Bürosoftware (bspw. Excel) erledigt werden, da die Beschaffung einer Fachanwendung aufgrund der kleinen Fallmenge nicht rentiert. Die Anbindung von Bürosoftware an eine Nachvollziehbarkeitslösung ist komplex, da im Allgemeinen nicht von standardisierten Datenstrukturen ausgegangen werden kann.

Je grösser die Gemeinde ist, desto mehr zusätzliche IT-Systeme mit den entsprechenden Personendatensammlungen sind im Einsatz. In vielen Gemeinden sind zusätzliche Systeme im Bereich der Geschäfts- und Dokumentenverwaltung im Einsatz. Auch Fachsysteme im Bereich des Sozialwesens sind häufig. Diese Systeme werden je nach Anforderungen um weitere Fachanwendungen ergänzt. Grössere Städte haben denn auch eine zwei- oder dreistellige Anzahl von Personendatensammlungen analog zu den Kantonen[49].

Für die Nachvollziehbarkeitslösung bedeutet dies, dass durch die Anbindung der Gemeindelösungen einiger weniger Anbieter potenziell eine Vielzahl von Personendatensammlungen aus den Gemeinden angebunden werden könnten. Dies betrifft vor allem die kleineren und mittelgrossen Gemeinden.

5.4.4. Einordnung Mengengerüst und Relevanz für UZ13

Basierend auf den vorgängig aufgeführten Analysen ergibt sich zusammengefasst folgendes Mengengerüst an Datensammlungen mit Personendaten:

- Ca. 1’000 auf Bundesebene
- Ca. 100+ pro Kanton (26 Kantone) → einige tausend insgesamt
- Einige wenige bis einige hundert pro Gemeinde (ca. 2’200 Gemeinden) → im Bereich von einigen Tausend oder sogar Zehntausend

Summiert ergibt sich damit in der Schweiz eine geschätzte fünfstellige Anzahl von Datensammlungen, welche Personendaten enthalten.

---

[45] Jede Gemeinde führt ein Einwohnerregister mit einem minimalen Set an standardisierten Daten (vgl. Registerharmonisierungsgesetz sowie Merkmalskatalog BFS): https://www.bfs.admin.ch/bfs/de/home/register/personenregister/registerharmonisierung.html

[46] Wichtige Anbieter sind (alphabetisch geordnet):

Abacus AG: https://www.abacus.ch/produkte

Abraxas (ehemals VRSG): https://www.abraxas.ch/de/digitale-verwaltung

Axians Infoma: https://www.axians-infoma.ch/

Dialog Verwaltungs-Data AG: https://www.dialog.ch/

Dumo Informatik & Scanning AG: https://www.dumo.ch/produkte

Hürlimann Informatik AG: https://www.hi-ag.ch/

Innosolv AG (nest digital government): https://www.obt.ch/de/unsere-leistungen/it-dienstleistungen/nest-is-e/, https://www.innosolv.ch/produkt/innosolvcity/

NRM AG: https://www.nrmag.ch/nrmag/softwareloesungen/index.php

ocom (ehemals ruf): https://www.ocom.ch/software/gemeindesoftware

[47] Siehe auch Interview mit Dr. Konrad Walser von der Berner Fachhochschule: https://www.netzwoche.ch/news/2016-10-26/die-heterogenitaet-der-it-in-der-oeffentlichen-verwaltung

[48] Siehe auch: https://www.inside-it.ch/de/post/was-ist-los-im-markt-fuer-gemeinde-software-20170627

[49] Die Stadt Bern hat ein öffentlich einsehbares Register der Personendatensammlungen. Stand Januar 2021 sind 122 Personendatensammlungen aufgeführt. Siehe: https://datenregister-stadt-bern.ideso.ch/

Mengengerüst IT-Anwendungen:

- Ca. 1'000 auf Bundesebene
- Ca. 100+ pro Kanton (26 Kantone) → einige tausend insgesamt
- Auf Gemeindeebene dürften viele Standardlösungen im Einsatz sein

Summiert ergeben sich somit in der Schweiz geschätzt mehrere tausend verschiedene IT-Systeme, in welchen Personendaten verarbeitet werden. Diese könnten potenziell an eine Nachvollziehbarkeitslösung angebunden[50] werden.

Diese Mengengerüste zeigen auf, dass eine flächendeckende Nachvollziehbarkeit mit der aktuellen IT-Landschaft von vielen verschiedenen dezentralen Anwendungen und teilweise manueller Datenverwaltung (bspw. Excel) schwierig und nur mit unverhältnismässig grossem Aufwand umsetzbar ist. Rechtliche, organisatorische und politische Aspekte erhöhen die Komplexität weiter. Es ist davon auszugehen, dass die Datenstrukturen und Dateninhalte in den verschiedenen Systemen nur teilweise standardisiert und harmonisiert sind.

Die vorhergehende Diskussion zeigt auf, welche Vielfalt an Anwendungen vorhanden ist. Wichtig ist aber auch deren Relevanz zu berücksichtigen, wie folgendes Beispiel exemplarisch zeigt:

- Die Applikation Infostar zur Pflege und Beurkundung sämtlicher Zivilstands-Ereignisse in der Schweiz enthält Informationen von nahezu allen Personen mit Schweizer Bürgerrecht sowie von Personen mit einem Zivilstands-Ereignis in der Schweiz. Aufgrund der grossen Anzahl betroffener natürlicher Personen dürfte das Interesse natürlicher Personen an einer Anbindung dieser Applikation an die Nachvollziehbarkeitslösung gross ausfallen.
- Im Bereich Feuerwerk und Sprengstoffe wird ein Register mit sämtlichen ausgegebenen Ausweisen geführt, welche zur Verwendung von Feuerwerk und Sprengstoffen ermächtigen[51]. Hier sind einerseits wenige Personen betroffen und diese wissen im Allgemeinen gut darüber Bescheid, dass sie in der entsprechenden Datenbank erfasst sind.

5.4.5. Exemplarische Auswahl von Systemen zur Bearbeitung von Personendaten

Wie vorgängig beschrieben, existiert eine grosse Anzahl von Systemen, in welchen durch die öffentliche Verwaltung auf den verschiedenen Staatsebenen Personendaten gespeichert und verarbeitet werden. Es würde den Rahmen dieser Studie sprengen, diese Systeme systematisch aufzulisten.

Basierend auf dem Register des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB)[52] wurde in Tabelle 3 exemplarisch ein erster Versuch unternommen, mögliche Systeme zu identifizieren, welche Personendaten von einer Vielzahl von natürlichen Personen enthalten. Diese Liste wurde exemplarisch durch Systeme aus den Kantonen ergänzt. Die Liste ist als Inspirationsquelle gedacht und erhebt keinen Anspruch auf Vollständigkeit oder darauf, die Systeme basierend auf den «richtigen» Kriterien identifiziert zu haben.

[50] Es stehen keine Informationen zur Verfügung, ob die Systeme technisch geeignet sind und welcher Aufwand für eine systemseitige Einbindung betrieben werden müsste.

[51] Siehe: https://www.fedlex.admin.ch/eli/cc/2001/78/de und https://www.sbfi.admin.ch/sbfi/de/home/bildung/sprengwesen/spreng--und-verwendungsausweise/berechtigungen-fwa--fwb--bf.html

[52] https://www.datareg.admin.ch/

Tabelle 3: Exemplarische Auswahl von Systemen mit Personendaten

Register, zufällig sortiert	Eigentümer
Register für administrative Identifikation von natürlichen Personen (AHVN13)	EFD - Zentrale Ausgleichsstelle ZAS
Versichertenregister	EFD - Zentrale Ausgleichsstelle ZAS
INFOSTAR - elektronisches Zivilstandsregister	EJPD - BJ - Eidgenössische Amt für das Zivilstandswesen
Einwohnerregister (harmonisiert)[53]	26 Kantone / ca. 2200 Gemeinden
Stimmregister (harmonisiert)[54]	26 Kantone / ca. 2200 Gemeinden
Register Steuerveranlagung Direkte Bundessteuer der natürlichen und juristischen Personen	EFD – ESTV
Kantonales Steuerregister (nicht harmonisiert)[55]	26 Kantone / ca. 2200 Gemeinden
Familienzulagenregister	EFD - Zentrale Ausgleichsstelle ZAS
Rentenregister	EFD - Zentrale Ausgleichsstelle ZAS
ZEMIS - Zentrales Migrationsinformationssystem	EJPD - Staatssekretariat für Migration
Zentrales Ausländerregister (ZAR)	EJPD - Staatssekretariat für Migration
Informationssystems für die Auszahlung von Leistungen der Arbeitslosenversicherung (ASAL)	WBF - SECO
AVAM (Arbeitsvermittlung und Arbeitsmarktstatistik)	WBF - SECO
Erwerbsersatzordnung-Register	EFD - Zentrale Ausgleichsstelle ZAS
Fingerabdruck-Datenbank AFIS	EJPD - fedpol
PISA (Personalinformationssystem der Armee)	VBS
Strafregister (VOSTRA)	EJPD - BJ
eVera (elektronische Verwaltung Auslandschweizer)	EDA
Register der Ergänzungsleistungen	EFD - Zentrale Ausgleichsstelle ZAS
EDNA (DNA-Profil-Erkennungsdienstliches Informationssystem	EJPD - fedpol
Sachleistungsregister (Ausgabe von Sachleistungen für AVH-Bezüger)	EFD - Zentrale Ausgleichsstelle ZAS
AUPER2 (Automatisches Personenregistratursystem Asylsuchende, Flüchtlinge, ...)	EJPD - Staatssekretariat für Migration
Betreibungsregister (nicht harmonisiert)	26 Kantone, ggf. mehrere pro Kanton
Register Verlustscheinverzeichnis	EFD - ESTV
Individuelles Konto (AHV)	Verteilt auf 26 kantonale Ausgleichskassen, rund 65 Verbandsausgleichskassen, Eidgenössische Ausgleichskasse und Schweizerische Ausgleichskasse

[53] Einwohnerregister gibt es sowohl auf Gemeindeebene als auch auf kantonaler Ebene (als Zusammenzug der Gemeinderegister).

[54] Das Stimmregister existiert nicht dauerhaft, sondern wird im Allgemeinen für jede Abstimmung neu basierend auf dem Einwohnerregister neu generiert. Es gibt jedoch gewisse Softwarelösungen, welche das Stimmregister dauerhaft basierend auf dem Einwohnerregister führen und aktualisieren.

[55] Die Steuerregister werden teilweise auf Gemeindeebene und/oder teilweise auf Kantonsebene geführt.

5.4.6. Datenaustausch und Datenzugriff zwischen den Verwaltungseinheiten am Beispiel ZEMIS

Nicht nur die grosse Anzahl verschiedener IT-Systeme, sondern auch die Vernetzung zwischen den Verwaltungseinheiten ist ein Komplexitätstreiber. Bei vielen Datensammlungen und den dazugehörigen IT-Systemen ist ein Zugriff auf die Daten sowie ein Datenaustausch mit anderen Organisationseinheiten der öffentlichen Verwaltung vorgesehen und umgesetzt. Exemplarisch wird dies hier am System «ZEMIS» (zentrales Migrationssystem) erläutert, da bei diesem in der «ZEMIS Verordnung SR 142.513» die Zugriffsrechte auf die Daten explizit aufgelistet sind[56]. Insgesamt dürfen 22 weitere Gruppen von Organisationseinheiten des Bundes und der Kantone[57] neben dem Systemeigentümer SEM (Staatssekretariat für Migration) auf das ZEMIS-System zugreifen. Werden die kantonalen Organisationseinheiten einzeln gezählt (bspw. 26 «kantonale Steuerbehörden»), so ergeben sich mehr als 100 verschiedene Organisationseinheiten der öffentlichen Verwaltung der Schweiz, welche auf das ZEMIS-System zugreifen können.

5.5. Grundlagen

5.5.1. Standardisierung der Systeme gemäss eCH

Für die mögliche Anbindung von Quellsystemen an eine Nachvollziehbarkeitslösung spielt nicht nur deren Menge eine Rolle, sondern auch, ob diese standardisiert sind. Verfügen verschiedene Systeme über gleiche standardisierte Schnittstellen, so vereinfacht sich eine mögliche Anbindung an eine Nachvollziehbarkeitslösung.

Über den Verein eCH[58] gibt es Standardisierungsbestrebungen für die Prozesse und die IT-Systeme der Schweizer Verwaltung auf allen drei Staatsebenen. Die eCH-Standards hatten bisher grundsätzlich einen empfehlenden Charakter. Mit der Rahmenvereinbarung zur E-Government-Zusammenarbeit in der Schweiz 2020 haben sich Bund, Kantone und Gemeinden neu dazu verpflichtet, die Standards des Vereins eCH in der Regel für verbindlich zu erklären – insbesondere bei Beschaffungen und Lösungsentwicklungen.

eCH hat bis heute in verschiedenen Fachbereichen Standards definiert. Die Standards decken jedoch immer nur einen Teil des Fachbereichs ab und fokussieren oftmals auf Prozesse und Schnittstellen und weniger auf die Datenhaltung. Es gibt auch verschiedene Fachbereiche in welchen Standardisierungen durch eCH für Personendaten bis jetzt komplett fehlen. Eine Vielzahl der Systeme zur Verarbeitung von Personendaten in der öffentlichen Verwaltung und der darin enthaltenen Daten sind daher nicht standardisiert. Weitere Details sind in Anhang A.6 aufgeführt.

5.5.2. Fehlende «Enabler»

Der «eGovernment Benchmark» der EU definiert den Begriff «Enabler», welcher digitale Bausteine bezeichnet, welche für E-Government Vorhaben als Grundlage dienen. Auch eine Nachvollziehbarkeitslösung hängt von solchen E-Government Bausteinen ab. Diverse dieser Enabler fehlen aktuell in der Schweiz, was die Umsetzung einer Nachvollziehbarkeitslösung erschwert. Die Folgende Tabelle 4 zeigt eine Übersicht über wichtige fehlende Enabler sowie deren potentielle Auswirkungen auf die Umsetzbarkeit einer Nachvollziehbarkeitslösung:

---

[56] In Anhang 1 der ZEMIS-Verordnung ist detailliert aufgelistet, welche anderen Organisationseinheiten welche Daten-Inhalte abfragen («A»), welche Organisationseinheiten die Daten bearbeiten («B») und welche Organisationseinheiten die Daten weitergeben dürfen («W»). Siehe: https://www.fedlex.admin.ch/eli/cc/2006/303/de

[57] Hier wurden die kantonalen Organisationseinheiten (bspw. «kantonale und kommunale Polizeibehörden») als «1 Gruppe von Organisationseinheiten» gezählt.

[58] Siehe: https://www.ech.ch

Tabelle 4: Wichtige E-Government Enabler, welche ganz oder teilweise fehlen.

Fehlender / nur teilweise vorhandener Enabler	Aktueller Stand sowie mögliche Auswirkungen auf eine Nachvollziehbarkeitslösung
National anerkannte E-ID	Die Abstimmung zur nationalen E-ID wurde im März 2021 abgelehnt. Es laufen diverse Aktivitäten, um das Thema der nationalen E-ID vorwärts zu bringen. Es ist wichtig, dass Personendaten sowie die dazugehörenden Metadaten von einer Nachvollziehbarkeitslösung lediglich der befugten natürlichen Person zur Verfügung gestellt werden. Es braucht daher eine vertrauenswürdige Art der Authentifikation der natürlichen Person gegenüber dem IT-System einer Nachvollziehbarkeitslösung.
Verwaltungsweit einheitliches Datenmanagement (Standardisierung & Harmonisierung von Daten)	Mit dem Programm NaDB (Nationale Datenbewirtschaftung) unter der Leitung des BFS werden erste Schritte zu einem harmonisierten Datenmanagement in der Verwaltung über alle drei föderalen Ebenen hinweg unternommen[59]. Wenn einer natürlichen Person Daten aus verschiedenen Systemen mittels einer Nachvollziehbarkeitslösung bereitgestellt werden sollen, so müssen gleiche oder ähnliche Daten (beispielsweise Adressen) aus verschiedenen Systemen aggregiert werden können. Ist dies nicht der Fall, so wird es schwierig sein, der natürlichen Person ihre Daten in einer verständlichen Form zu präsentieren. Eine Aggregation von gleichen oder ähnlichen Daten aus verschiedenen Systemen ist aufwändig, solange diese verschiedenen Systeme sich nicht an ähnliche Standards in der Datenhaltung und der Datenmodellierung halten.
Verwendung einheitlicher und eindeutiger Identifikatoren	Neu wird die systematische Verwendung der AVHN13 (AHV-Nummer) in verschiedenen Systemen möglich sein. Damit steht ein potenzieller eindeutiger Identifikator bereit, welcher dann in verschiedenen Systemen verwendet werden könnte. Ein Datensatz muss eindeutig mit einer natürlichen Person verknüpft werden können. Ansonsten kann der Datenschutz nicht sichergestellt werden. Einheitliche Identifikatoren erlauben es, Datensätze einer natürlichen Person über verschiedene Systeme hinweg eindeutig zuzuordnen.
E-Government Portal(e) für natürliche Personen	Für Unternehmen wurde das zentrale Portal easygov.swiss etabliert. Auf Bundesebene fehlt aktuell ein ähnliches Portal für natürliche Personen. Diverse Kantone setzen E-Government Portale ein. Für eine Nachvollziehbarkeitslösung muss eine Web-Oberfläche bereitgestellt werden, um den natürlichen Personen Zugriff auf ihre Personendaten sowie die Nachvollziehbarkeits-Informationen zu gewähren. Ein bestehendes E-Government Portal wäre eine naheliegende Option, um solche Informationen bereitzustellen.

5.5.3. Plattformen zum Datenaustausch

Plattformen zum Datenaustausch könnten an eine Nachvollziehbarkeitslösung angebunden werden. Sofern die Datenplattform den Austausch von Daten zwischen Verwaltungseinheiten mitlesen kann, könnte diese Information natürlichen Personen über die Nachvollziehbarkeitslösung zur Verfügung gestellt werden. In der Schweiz ist «sedex» für den Datenaustausch mit der öffentlichen Verwaltung sowie innerhalb der öffentlichen Verwaltung weit verbreitet. Insbesondere sind sämtliche Kantone und Gemeinden an sedex angeschlossen. sedex ist Ende-zu-Ende verschlüsselt: Lediglich der Absender und der Empfänger der Nachricht kennen deren Inhalt[60]. sedex ist daher in

[59] Beispielsweise im Bereich der Geodaten sind entsprechende Massnahmen eines vereinheitlichten Datenmanagements bereits weiter fortgeschritten – diese sind im Scope von UZ13 mit Fokus auf Personendaten aber weniger relevant.

[60] Die Ende-zu-Ende-Verschlüsselung ist ein bewusst gewähltes «Feature» von sedex, um den Datenschutz sicherzustellen. Technisch ist sedex oftmals so implementiert, dass die Nachricht vom sendenden Fachsystem unverschlüsselt an den dazugehörenden sedex-Adapter geliefert wird, dieser die Nachricht verschlüsselt an den sedex-Adapter des Empfängersystems sendet. Der sedex-Empfänger entschlüsselt dann die Nachricht, prüft diese gegebenenfalls und liefert diese ans empfangende Fachsystem weiter. Details dazu auch im sedex Betriebshandbuch: https://www.bfs.admin.ch/bfsstatic/dam/assets/315862/master

der heutigen Form nicht geeignet, um einer Nachvollziehbarkeitslösung Informationen über den Datenaustausch zwischen verschiedenen Verwaltungseinheiten zu liefern. Im Bereich des Lohnmeldewesens ist in der Schweiz «ELM» im Einsatz und im Bereich der Medizindaten ist «HIN» relativ weit verbreitet. In Europa werden zudem die beiden Systeme «X-Road» und «eDelivery» eingesetzt.

Weitere Details zu diesen Plattformen sind in Anhang A.7 aufgeführt. Es ist in jedem Einzelfall zu prüfen, ob die technische Möglichkeit besteht, eine Plattform zum Datenaustausch an eine Nachvollziehbarkeitslösung anzubinden.

5.6. Erfahrungen aus anderen Vorhaben

5.6.1. Umsetzung der Nachvollziehbarkeitsfunktion in Dänemark, Estland und Luxemburg

Dieser Abschnitt fasst exemplarisch Beispiele von anderen Ländern zusammen, in welcher eine digitale Lösung zur Nachvollziehbarkeit der Verwendung von Personendaten bereits umgesetzt wurde oder deren Umsetzung geplant ist[61]. Details dazu sind in Anhang A.8 aufgeführt.

- **Dänemark** plant aktuell einen umfassenden und zentralisierten Online-Schalter für digitale Behördengänge (borger.dk / «mit overblik»). Es ist angedacht, eine Nachvollziehbarkeits-Funktion zu erstellen – deren Umfang und Funktionalität ist aktuell aber noch unklar.
- **Estland** bietet seinen Bürgern einen Zugriffslog auf vier ausgewählte und besonders relevante Datenbanken an (Funktion «Data Tracker» als Teil von «X-Road»).
- **Luxemburg** bietet seinen Bürgern einen Online-Schalter («myguichet.lu») für Interaktionen mit der öffentlichen Verwaltung an. Teil des Online-Schalters ist ein Zugriffslog auf das Personenregister. Per Brief dürfen Bürger zudem Auskunft verlangen, für welchen Zweck ein Datenzugriff durchgeführt wurde.

Es fällt auf, dass die «Nachvollziehbarkeits-Funktion» in oben genannten Ländern ein «Zusatz-Feature» zu anderen E-Government-Dienstleistungen darstellt und stark auf diesen aufbaut. Keines der drei Länder hat die «Nachvollziehbarkeits-Funktion» als reinen Selbstzweck umgesetzt. Ebenfalls wurde die «Nachvollziehbarkeits-Funktion» lediglich für eine Auswahl von wenigen besonders relevanten und zentralisierten Datenbanken umgesetzt.

Weiter ist zwingend eine staatlich anerkannte und verifizierte Form der digitalen Personen-Authentifizierung notwendig – in den oben genannten Beispielen wird jeweils die nationale elektronische Identität verwendet.

Die Umsetzung wurde in den oben genannten Beispielen von der Zentralregierung geleitet. Im Beispiel von Dänemark und Luxemburg wurden zudem die Regionen / Kantone sowie die Gemeinden eng in die Umsetzung eingebunden. Selbstverständlich basierte die Umsetzung auf den notwendigen gesetzlichen Grundlagen, welche entsprechend geschaffen werden mussten.

5.6.2. Fallbeispiel: Elektronisches Patientendossier (EPD)

Im elektronischen Patientendossier der Schweiz (EPD) wurde ein Teil der Anforderungen, welche an eine Nachvollziehbarkeitslösung gestellt werden könnten, umgesetzt:

- Natürliche Personen können die Log-Dateien sämtlicher Zugriffe auf ihre persönlichen im elektronischen Patientendossier abgelegter Dateien einsehen[62]. Die Log-Dateien müssen 10 Jahre lang gespeichert werden[63].

[61] Den Autoren der Studie sind keine weiteren Länder bekannt, welche eine entsprechende Nachvollziehbarkeitslösung anbieten. Es kann jedoch nicht ausgeschlossen werden, dass weitere Länder ein solches Angebot haben oder daran sind, dieses aufzubauen.

- Natürliche Personen müssen Zugriffe auf persönliche Daten explizit freigeben[64].
- Natürliche Personen können jederzeit die Löschung einzelner Daten verlangen[65].

Das elektronische Patientendossier ist ein in sich geschlossenes «Sekundär-System»: Die medizinische Fachkraft bearbeitet die Daten auf dem jeweiligen Primär-System (bspw. im Spital, in der Arztpraxis). Bei Abschluss der Behandlung werden die daraus generierten Dokumente im elektronischen Patientendossier abgelegt. Gibt die natürliche Person ein Dokument aus seinem elektronischen Patientendossier einer medizinischen Fachkraft frei, so kann diese das Dokument wiederum auf das eigene Primärsystem laden. Zugriffe werden lediglich dann geloggt, wenn diese direkt auf dem Patientendossier stattfinden. Zugriffe auf den verschiedenen Primärsystemen werden per Definition nicht durch das elektronische Patientendossier geloggt.

Das erste Patientendossier wurde im Dezember 2020[66] eröffnet. Zur Eröffnung eines elektronischen Patientendossiers muss sich die natürliche Person vorgängig persönlich bei einer zertifizierten Stelle registrieren. Das elektronische Patientendossier ist aktuell in der Schweiz noch nicht flächendeckend verfügbar, weshalb sich noch keine Aussagen zur Akzeptanz und der Verwendung der Log-Funktion machen lassen.

Technisch basiert das Logging auf dem international verwendeten ATNA[67] Protokoll. Zugriffe (auch technische Zugriffe durch das System selbst) werden ausführlich geloggt. Zugriffe werden personenscharf geloggt und den jeweiligen Besitzern des Patientendossiers angezeigt. Um die hohen Anforderungen des Datenschutzes zu gewährleisten, finden zudem regelmässige und umfangreiche Audits statt.

Die natürliche Person, welcher das Dossier gehört, muss für jedes Dokument eine Kategorisierung angeben (einsehbar, nur mit Erlaubnis einsehbar, geheim). Zudem muss die natürliche Person explizite Zugriffsberechtigungen vergeben (an Einzelpersonen, Organisationseinheiten oder Organisationen), sodass das behandelnde Gesundheitspersonal Zugriff auf die entsprechenden Dokumente erhält. In der Praxis gestaltet sich diese Zugriffsvergabe aktuell aufgrund der hohen Komplexität schwierig, sodass Zugriffe oft nicht wie gewünscht von den natürlichen Personen gesetzt werden. Die Möglichkeit, dass eine medizinische Fachkraft im Rahmen einer Untersuchung Zugriff auf ein Dokument des Dossiers bei Bedarf beantragen kann, fehlt aktuell. Nur in Notfällen darf berechtigtes medizinisches Fachpersonal einen Notfallzugang zum elektronischen Patientendossier beantragen.

Die Autoren der Studie konnten eine Implementierung des elektronischen Patientendossiers einsehen. Relevant für UZ13 ist dabei insbesondere, dass die präsentierten Log-Daten in der eingesehenen Implementierung nur schwer verständlich waren. Daraus abgeleitet ergibt sich, dass bei einer Implementierung einer Nachvollziehbarkeitslösung ein spezielles Augenmerk auf die Nutzerzentrierung gelegt werden muss.

---

[62] SR 816.11, Artikel 18 - Verordnung über das elektronische Patientendossier (https://www.fedlex.admin.ch/eli/cc/2017/204/de)

[63] SR 816.111, Anhang 2 der Verordnung des EDI vom 22. März 2017 über das elektronische Patientendossier, Kapitel 2 (Art. 10 Abs. 3 Bst. d EPDV)
https://www.bag.admin.ch/dam/bag/de/dokumente/nat-gesundheitsstrategien/strategie-ehealth/gesetzgebung-elektronisches-patientendossier/gesetze/Anhang_2_EPDV_EDI_20190624.pdf.download.pdf/Anhang%202%20der%20EPDV-EDI_Fassung%20vom%2024.%20Juni%202019.pdf)

[64] SR 816.111, Anhang 2 der Verordnung des EDI vom 22. März 2017 über das elektronische Patientendossier, Kapitel 9 (Art. 18 Bst. a EPDV)
https://www.bag.admin.ch/dam/bag/de/dokumente/nat-gesundheitsstrategien/strategie-ehealth/gesetzgebung-elektronisches-patientendossier/gesetze/Anhang_2_EPDV_EDI_20190624.pdf.download.pdf/Anhang%202%20der%20EPDV-EDI_Fassung%20vom%2024.%20Juni%202019.pdf
Für Notfälle bestehen spezifische Regelungen (Kapitel 2.2)

[65] SR 816.11, Artikel 10 - Verordnung über das elektronische Patientendossier (https://www.fedlex.admin.ch/eli/cc/2017/204/de)

[66] https://www.srf.ch/news/schweiz/digitalisierung-der-gesundheit-erstes-elektronisches-patientendossier-der-schweiz-eingefuehrt

[67] Audit Trail and Node Authentication

6. Der Lösungsraum für mögliche Umsetzungen der Nachvollziehbarkeit der Verwendung von Personendaten durch die öffentliche Verwaltung

6.1. Schlüsselerkenntnisse

Damit eine **Nachvollziehbarkeitslösung erfolgreich umgesetzt** werden kann, muss eine **Balance** zwischen den verschiedenen **Anforderungen** und **Erwartungen** gefunden werden:

- Eine Nachvollziehbarkeitslösung muss die **Bedürfnisse** der **natürlichen Personen** möglichst gut erfüllen. Sei dies bei der Bereitstellung der relevanten Informationen, bei der Benutzerfreundlichkeit oder bei der Auswahl der relevanten Quellsysteme. Zentral dabei ist, dass die Information zur Nachvollziehbarkeit so aufbereitet wird, dass natürliche Personen diese verstehen.
- Die Nachvollziehbarkeitslösung muss von der **Politik** und der **Gesellschaft akzeptiert** werden. Es ist insbesondere sicherzustellen, dass die Nachvollziehbarkeitslösung keine Daten auf Vorrat sammelt und dass die föderale Aufgabenteilung respektiert wird.
- Für die Akzeptanz der Nachvollziehbarkeitslösung ist es ebenfalls wichtig, dass die **Bedürfnisse** der **öffentlichen Verwaltung** berücksichtigt werden.
- Eine Nachvollziehbarkeitslösung muss **geltendes Recht respektieren**. Bei Bedarf können zusätzliche rechtliche Grundlagen geschaffen werden (wobei für diese wiederum die politische Akzeptanz notwendig ist).
- Eine Nachvollziehbarkeitslösung – insbesondere in einer skalierten Umsetzung – stellt je nach Lösungsvariante viele Personendaten zum einfachen Online-Zugriff zur Verfügung. Der **Datenschutz** und die **Datensicherheit** sind **zwingend** sicherzustellen.
- Die Umsetzung einer Nachvollziehbarkeitslösung stellt je nach Variante unterschiedliche **Anforderungen** an die **Quellsysteme** bezüglich dem **Logging** von Zugriffen, der **Qualität** der Datenhaltung und auch der Anpassung von **Prozessen**. Die Aggregation von Daten und Zugriffen muss auf Systemebene definiert werden und sollte sich an noch zu definierenden Standards orientieren. Beim Logging der Zugriffsgründe ist einerseits darauf zu achten, dass diese für natürliche Personen verständlich sind und andererseits, dass dadurch die Prozesse der Verwaltung nicht unnötig durch zusätzlichen Aufwand belastet werden.
- Eine **skalierbare Nachvollziehbarkeitslösung** braucht eine **Systemarchitektur** sowie definierte **Schnittstellen**. Die Nachvollziehbarkeitslösung kann mittels eines zentralen Systems, mittels verschiedener föderierter Systeme oder mittels dezentralen Systemen umgesetzt werden. Aus politischer Sicht ist fraglich, ob ein stark zentralisiertes System heute mehrheitsfähig wäre. Das Schaffen von **Standards** kann dabei unterstützen, längerfristig ein möglichst homogenes Gesamtsystem zu erhalten.
- Je **kleiner** der **Umfang** einer Nachvollziehbarkeitslösung (in angebotenen Informationen, Funktionalitäten und angeschlossenen Quellsystemen) ist, desto **schneller** ist diese **umsetzbar**. Im Gegenzug wird dadurch der **Nutzen** für natürliche Personen möglicherweise **beschränkt**.

Eine Nachvollziehbarkeitslösung muss sich zudem in verschiedene existierende Rahmenbedingungen eingliedern. Diese Rahmenbedingungen sind nicht starr, sondern entwickeln sich mit der Zeit.

6.2. Verschiedene Themengebiete, welche es bei der Umsetzung einer Nachvollziehbarkeitslösung zu berücksichtigen gibt

Damit eine Nachvollziehbarkeitslösung zum Erfolg wird, müssen eine Vielzahl von Anforderungen berücksichtigt werden. Eine Übersicht über verschiedene relevante Themengebiete ist in Abbildung 6 dargestellt. Die Themengebiete sind im Folgenden kurz vorgestellt:

Natürliche Personen & Bedürfnisse	Damit mit der Nachvollziehbarkeitslösung Transparenz im Sinne der Vision von UZ13 erzeugt werden kann, müssen die Bedürfnisse der natürlichen Personen abgedeckt werden.
Anwendungsfälle	Die Bedürfnisse von natürlichen Personen können im Allgemeinen nicht global erfüllt werden, sondern lediglich für konkrete Anwendungsfälle.
Politik & Akzeptanz	Die Nachvollziehbarkeitslösung, welche umgesetzt werden soll, muss politisch und gesellschaftlich mehrheitsfähig sein.
Bedürfnisse der öffentlichen Verwaltung	Die öffentliche Verwaltung möchte mit der Nachvollziehbarkeitslösung ebenfalls Ziele erreichen, welche für eine erfolgreiche Umsetzung berücksichtigt werden müssen.
Umsetzung	Die Nachvollziehbarkeitslösung muss im Rahmen von einem oder mehreren Vorhaben umgesetzt werden.
Gesetze & Verordnungen	Je nach gewählter Lösungsvariante sind kleinere oder grössere Anpassungen oder Erweiterungen von bestehenden Gesetzen und Verordnungen notwendig. Bestehende Gesetze und Verordnungen sind als Rahmenbedingungen zu berücksichtigen.
Daten	Daten stehen im Zentrum einer möglichen Nachvollziehbarkeitslösung: Entweder als Personendaten selbst oder als Metadaten bezüglich der Verwendung von Personendaten.
Anzuschliessende Quellsysteme[68]	Um Transparenz in der Nutzung von Personendaten zu erzeugen, müssen die relevanten Quellsysteme angeschlossen werden, in welchen Personendaten gespeichert, verarbeitet und auf diese zugegriffen wird.
Prozesse & Leistungen	Personendaten werden von der öffentlichen Verwaltung im Rahmen von Prozessen und Leistungen erhoben und verarbeitet.
Architektur & Schnittstellen	Spätestens dann, wenn an die Nachvollziehbarkeitslösung verschiedene Quellsysteme angeschlossen werden sollen – i.e. die Lösung skalierbar sein soll - werden eine IT-Architektur und definierte Schnittstellen notwendig.
Betrieb & Weiterentwicklung	Eine einmal erschaffene Nachvollziehbarkeitslösung muss betrieben und weiterentwickelt werden.
Andere E-Government Vorhaben	Die Umsetzung anderer Vorhaben kann eine Umsetzung des Vorhabens der Nachvollziehbarkeit der Verwendung von Personendaten vereinfachen.

Viele dieser Anforderungen haben Abhängigkeiten zueinander und können nicht ohne weiteres getrennt voneinander betrachtet werden. Im Folgenden werden die verschiedenen Anforderungen dennoch separat voneinander betrachtet, ausgewählte Verweise auf wichtige Abhängigkeiten werden explizit aufgeführt.

[68] Der Begriff «Quellsystem» wird als Sammelbegriff für sämtliche Systeme verwendet, welche an eine Nachvollziehbarkeitslösung angeschlossen werden könnten.

Abbildung 6: Wichtige Themengebiete, welche bei einer Umsetzung einer Nachvollziehbarkeitslösung berücksichtigt werden müssen.

6.3. Natürliche Personen und ihre Bedürfnisse

Wie bereits in Kapitel 4 beschrieben, kann davon ausgegangen werden, dass natürliche Personen grundsätzlich einen Bedarf an (zusätzlicher) Transparenz im Bereich der Verwendung von Personendaten durch die öffentliche Verwaltung haben. Die Bedürfnisse dürften sich jedoch bei verschiedenen natürlichen Personen unterscheiden. Im Bereich der Nachvollziehbarkeitslösung kommt hinzu, dass es entsprechende Dienstleistungen aktuell nicht oder nur sehr begrenzt gibt, was möglicherweise dämpfend auf den aktuellen Bedarf wirkt[69].

6.3.1. Nutzerzentrierung als Schlüssel zum Erfolg

Um die Vision dieses Vorhabens – ein gesteigertes Vertrauen der natürlichen Personen in die öffentliche Verwaltung durch verbesserte Transparenz im Bereich der Verwendung von Personendaten – zu erreichen, ist eine konsequente Nutzerzentrierung unerlässlich. Das Thema Nutzerzentrierung ist umfangreich, weshalb hier exemplarisch einzelne ausgewählte Aspekte kurz beleuchtet werden:

Wie viel Aufwand muss eine natürliche Person betreiben, um an die Informationen zu gelangen?	Im Idealfall können natürliche Personen die Informationen zur Nachvollziehbarkeit der Verwendung ihrer Personendaten auf bereits genutzten Portalen einsehen. Jeder zusätzliche Schritt – beispielsweise der Besuch einer separaten Website oder ein kompliziertes Anmeldeverfahren – erschweren die Nutzung der bereitgestellten Informationen und reduzieren die Chance, dass die Vision erreicht werden kann.
Finden natürliche Personen die gesuchte Information?	Eine geeignete Strukturierung der Informationen sowie eine übersichtliche Benutzeroberfläche erleichtern es natürlichen Personen, die gesuchte Information zu finden. Auch Optionen zur Filterung nach Themenbereichen bieten eine Möglichkeit, die Informationen weiter zu strukturieren. Ein frühes und wiederholtes Testen der Benutzeroberfläche mit einer diversen und repräsentativen Nutzergruppe kann hier zum Erfolg führen.

[69] Das Angebot kann die Nachfrage stärken – das Smartphone ist ein gutes Beispiel dafür.

Verstehen die natürlichen Personen die präsentierte Information?	Mögliche Massnahmen sind die Wahl von einfacher Sprache, einer geeigneten Aufbereitung der Daten sowie einfach verständliche Texte, welche die präsentierten Informationen erläutern.
Bestehen einfache Möglichkeiten, um Rückfragen zu stellen und Verbesserungen vorzuschlagen?	Unabhängig davon, wie gut die Benutzeroberfläche gestaltet wird: Es wird immer den Fall geben, dass einzelne natürliche Personen Fragen zu den präsentierten Informationen haben. Wird der natürlichen Person ein einfach zugänglicher Kanal geboten, um ihre Frage zu stellen, kann diese Unsicherheit im Idealfall in Vertrauen in die öffentliche Verwaltung umgewandelt werden. Mindestens eine Kontaktadresse (analog oder digital) oder ein entsprechender Kommunikationskanal sollte bereitgestellt werden.
Welche Optionen bestehen, wenn Daten fehlerhaft sind?	Werden der natürlichen Person Daten angezeigt, welche von dieser als möglicherweise fehlerhaft erkannt werden, so sollte der natürlichen Person aufgezeigt werden, wie sie die Korrektur der Daten veranlassen kann.
Ist klar kommuniziert, was die natürliche Person von der Nachvollziehbarkeitslösung erwarten darf?	Erwartet die natürliche Person von der Nachvollziehbarkeitslösung Dinge, welche diese nicht leisten kann, so wird dadurch das Ziel der Vision nicht erreicht. Es sollte daher proaktiv und klar kommuniziert werden, was die Nachvollziehbarkeitslösung leisten kann und was nicht.

6.3.2. Den Bedarf von natürlichen Personen besser verstehen

Der generelle Bedarf von natürlichen Personen nach zusätzlicher Transparenz der Verwaltung im Umgang mit Personendaten ist dokumentiert (siehe auch Abschnitt 4.2). Es fehlen aktuell jedoch detaillierte Erkenntnisse darüber, welche Services oder Informationen einer Nachvollziehbarkeitslösung den grössten Mehrwert bringen würden.

Um weitere Erkenntnisse über den Bedarf von natürlichen Personen nach Transparenz zu erhalten, wurden verschiedene Fragen erarbeitet, welche im Rahmen der Schweizer E-Gov-Studie 2021 gestellt wurden. Die erarbeiteten Fragestellungen sind in Anhang A.13 aufgeführt. Die Resultate der E-Gov-Studie 2021 werden im Frühjahr 2022 nach Abschluss dieser Machbarkeitsstudie publiziert.

6.3.3. Verhindern, dass Vertrauen zerstört wird

Eine schlecht umgesetzte Nachvollziehbarkeitslösung hat das Potenzial Vertrauen zu zerstören. Mögliche Szenarien (nicht abschliessend) sind:

- Die natürliche Person versteht die präsentierte Information nicht, weil diese nicht zielgruppengerecht aufbereitet wurde.
- Die natürliche Person ist von der Menge der Datensammlungen derart überrascht, dass die Nachvollziehbarkeitslösung das Vertrauen mindestens kurzfristig senkt.
- Die natürliche Person ist überrascht, wer alles Zugriff auf die jeweiligen Personendaten hat und empfindet dies als unangebracht, ungerechtfertigt oder unnötig.
- Die natürliche Person sieht einen Datenzugriff, welchen sie nicht nachvollziehen kann. Eine Nachfrage bei der zugreifenden Verwaltungsstelle führt nicht zu einer Klärung der Sachlage.
- Die von der Nachvollziehbarkeitslösung angebotenen Informationen werden als «Schein-Transparenz» interpretiert, indem nur Informationen aus wenigen ausgewählten Quellsystemen präsentiert werden.

- Die natürliche Person findet auf der Nachvollziehbarkeitslösung die erwarteten Informationen nicht.

Es ist daher wichtig, dass eine Nachvollziehbarkeitslösung ausgiebig und mit einer diversen Nutzergruppe getestet wird, bevor diese in den ordentlichen Betrieb geht (siehe auch obenstehenden Abschnitt zur Nutzerzentrierung). Geeignete begleitende Kommunikationsmassnahmen sowie Schulungen auf Seite der Verwaltung werden empfohlen.

6.4. Anwendungsfälle

Mit dem Begriff des «Anwendungsfalls» wird beschrieben, welche Information eine natürliche Person von einer Nachvollziehbarkeitslösung erhält. Die Anwendungsfälle sind im Detail in Kapitel 7 beschrieben, da diese für die Diskussion des weiteren Vorgehens zentral sind.

6.5. Politik & Akzeptanz

Eine fundierte Aussage darüber, welche Lösungsansätze politisch und gesellschaftlich eine Mehrheit finden, ist im Vornherein schwierig abzugeben. Basierend auf vergangenen politischen Diskussionen und Volksabstimmungen[70] lassen sich dennoch gewisse Tendenzen erkennen. Im Folgenden wird daher ein Versuch durch die Autoren der Studie unternommen, wichtige Aspekte zu beleuchten, welche bei einer möglichen Umsetzung einer Nachvollziehbarkeitslösung zu berücksichtigen sind:

Föderalismus respektieren	Die Schweiz besitzt ein föderales System, welches wiederholt bestätigt wurde. Ein Lösungsansatz für die Nachvollziehbarkeit der Verwendung von Personendaten muss dieser Tatsache Rechnung tragen. Eine verstärkte Zentralisierung verbunden mit einer Verschiebung von Aufgaben und Kompetenzen von Gemeinden, Kantonen und Bund könnte politisch einen schweren Stand haben[71].
Kein Datensammeln auf Vorrat / kein gläserner Bürger	Bei der Wahl einer Lösungsarchitektur sollte darauf geachtet werden, dass nicht unnötig Daten – ggf. sogar zentral – auf Vorrat gesammelt werden. Ansonsten könnte der Eindruck entstehen, dass die öffentliche Verwaltung unter dem Vorwand der Schaffung von Transparenz einen neuen «Datentopf» zur Schaffung des «gläsernen Bürgers» aufbauen möchte.
Datensicherheit ist zentral	Sobald bei einer Nachvollziehbarkeitslösung Personendaten oder Metadaten zu Personendaten ausgetauscht, gespeichert oder auch nur angezeigt werden, ist auf eine hohe Datensicherheit zu achten. Dies, da diese Daten bei Verwendung durch unbefugte Akteure ein hohes Missbrauchspotential haben können.
Keine Schwächung des Datenschutzes	Mit der Umsetzung einer Nachvollziehbarkeitslösung darf der Datenschutz nicht geschwächt werden. Die Nachvollziehbarkeitslösung sollte nicht dazu führen, dass Verwaltungseinheiten (oder Dritte) zusätzliche Möglichkeiten zum Zugriff auf Personendaten (oder daraus abgeleiteten Metadaten) erhalten. Da Personendaten involviert sind, ist der frühzeitige Einbezug des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) zwingend.

[70] Abstimmung zur E-ID, Überarbeitung Datenschutzgesetz, übergreifende Verwendung der AHVN13, …

[71] Eine allfällige Zentralisierung könnte durchaus Vorteile durch Synergiegewinnung haben. Eine allfällige Zentralisierung von Aufgaben ist in erster Linie eine politische Fragestellung und beschränkt sich bei weitem nicht nur auf eine Nachvollziehbarkeitslösung im Sinne von UZ13.

Nachvollziehbarkeitslösung mit Fokus auf die öffentliche Verwaltung	Die Abstimmung zur E-ID hat gezeigt, dass eine Nachvollziehbarkeitslösung mit Einbezug von Systemen aus der Privatwirtschaft einen schweren Stand haben dürfte. Die Nachvollziehbarkeitslösung soll sich daher – mindestens in einem ersten Schritt – auf Quellsysteme der öffentlichen Verwaltung beschränken.
Kosten und Nutzen	Die Umsetzung einer Nachvollziehbarkeitslösung kostet Geld. Je grösser die Kosten sind und je kleiner der empfundene Mehrwert einer Nachvollziehbarkeitslösung ist, desto geringer wird die Akzeptanz für diese ausfallen.
Einbezug wichtiger Stakeholder	Um eine Nachvollziehbarkeitslösung erfolgreich umsetzen zu können, müssen die relevanten Stakeholder frühzeitig involviert werden.

6.6. Bedürfnisse der Verwaltung

Auch die öffentliche Verwaltung hat Bedürfnisse, welche im Rahmen einer Nachvollziehbarkeitslösung berücksichtigt werden müssen. Dies sind beispielsweise:

Mehraufwände verhindern	Das Logging der Zugriffe auf die Daten inklusive der Begründung für den Zugriff soll soweit als möglich automatisiert werden, um Mehraufwände zu verhindern. Die manuelle Eingabe eines Zugriffsgrundes ist auf ein Minimum zu beschränken.
Aufzeigen, dass Vorgaben eingehalten werden	Mit der Nachvollziehbarkeitslösung möchten die verschiedenen Organisationseinheiten gegenüber den natürlichen Personen aufzeigen können, dass die geltenden Vorgaben vollumfänglich eingehalten werden.
Unterstützung bei der Umsetzung	Die Nachvollziehbarkeit soll möglichst über alle föderalen Ebenen und über fachliche Grenzen hinweg einheitlich umgesetzt werden. Um die Betreibenden von Quellsystemen bei der Umsetzung der Nachvollziehbarkeit beispielsweise im Rahmen des Life-Cycles zu unterstützen, könnte ein Leitfaden zur Verfügung gestellt werden. Hierbei sind verschiedene Themen von der Architektur über das Aufbereiten der Daten bis hin zu den rechtlichen Grundlagen zu berücksichtigen.
Klare Vision aufzeigen	Das gewünschte Ziel insbesondere auch im Zusammenspiel mit anderen E-Government Vorhaben (bspw. Portale, E-ID, …) soll klar aufgezeigt werden. Dies ermöglicht es den Betreibenden der Quellsysteme ein klares Zielbild zu verfolgen.

6.7. Umsetzung

Es gibt verschiedene Varianten, wie eine Nachvollziehbarkeitslösung umgesetzt werden könnte. Das Kapitel 8 präsentiert verschiedene Ansätze.

6.8. Gesetze und Verordnungen

Die Umsetzung einer Nachvollziehbarkeitslösung wird wahrscheinlich eine Anpassung oder Weiterentwicklung der Rechtsgrundlagen bedingen. Die Thematik der Rechtsgrundlagen wird losgelöst von diesem Dokument in einer separaten Rechtsgrundlagenanalyse betrachtet.

6.9. Daten

Daten und daraus abgeleitete Informationen sind das Kernstück einer Nachvollziehbarkeitslösung: Einerseits die Personendaten selbst und andererseits die dazugehörenden Metadaten zu den Zugriffen auf die Personendaten. Damit die Daten in einer für natürliche Personen verständlichen Form präsentiert werden können, müssen diese je nach Quellsystem aufbereitet und gegebenenfalls sogar über mehrere Datensammlungen hinweg aggregiert werden. Dabei stellen sich Anforderungen an die Datenhaltung (bspw. eindeutige Identifikatoren), die Standardisierung und Harmonisierung von Daten sowie und an die Datenqualität. Weitere Details sind in Anhang A.9 aufgeführt.

6.10. Anzuschliessende Quellsysteme

Je nach gewählter Lösungsvariante entstehen auf der Seite der anzuschliessenden Quellsysteme Anforderungen, welche umgesetzt werden müssen, damit das betreffende Quellsystem an eine Nachvollziehbarkeitslösung angebunden werden kann. Zentral ist dabei die Definition, welche Informationen das Quellsystem in welcher Granularität an die Nachvollziehbarkeitslösung liefern soll und wie Zugriffe geloggt werden (siehe auch Anhang A.10).

Quellsysteme können basierend auf verschiedensten Kriterien für die Anbindung an eine Nachvollziehbarkeitslösung priorisiert werden (siehe auch Abschnitt 8.5). Ist der Entscheid getroffen, dass ein Quellsystem an die Nachvollziehbarkeitslösung angeschlossen werden soll, müssen verschiedene Punkte beachtet werden:

- Die Granularität der einer natürlichen Person angebotenen Informationen muss definiert werden.
- Der Eigentümer des Quellsystems muss bereit sein, die notwendigen Anpassungen am Quellsystem (insbesondere das Logging der Zugriffe basierend auf den Anforderungen einer Nachvollziehbarkeitslösung und die Anbindung an eine Nachvollziehbarkeitslösung per Schnittstelle) durchzuführen, damit das Quellsystem an die Nachvollziehbarkeitslösung angeschlossen werden kann.
- Rechtliche Grundlagen für die Anbindung an eine Nachvollziehbarkeitslösung müssen vorhanden sein oder geschaffen werden.

6.11. Prozesse und Leistungen

Prozesse und Leistungen sind die Auslöser für Zugriffe auf Personendaten durch die öffentliche Verwaltung. Prozesse und Leistungen können natürlichen Personen gleichzeitig auch Kontext liefern, «weshalb» auf ihre Personendaten zugegriffen wurde. Um diesen Kontext natürlichen Personen im Rahmen einer Nachvollziehbarkeitslösung präsentieren zu können, müssen die entsprechenden Informationen im Rahmen der Bearbeitung der Prozesse und Leistungen erfasst werden. Dieser Schritt erzeugt einen Mehraufwand, wenn er nicht automatisiert wird.

Prozesse der öffentlichen Verwaltung sind heute oftmals eine Kombination von digitalen und analogen Prozessschritten. Auch wenn eine Tendenz zu mehr digitalen Prozessen und Prozessschritten sichtbar ist: Die Möglichkeit, Leistungen am physischen Schalter in Anwesenheit einer physischen Person zu beziehen oder anzustossen, wird so schnell nicht verschwinden. Es ist daher wichtig, dass im Rahmen der Umsetzung einer Nachvollziehbarkeitslösung auch die analogen Prozessschritte betrachtet werden. Weiter sollten die Mitarbeitenden beispielsweise am Schalter über die Nachvollziehbarkeitslösung geschult werden, um kompetent Auskunft geben zu können.

Werden natürlichen Personen zusätzliche Informationen zur Verwendung ihrer Personendaten durch die öffentliche Verwaltung im Rahmen einer Nachvollziehbarkeitslösung zur Verfügung gestellt, so kann dadurch ein Bedarf nach weiteren Dienstleistungen entstehen. Naheliegende

Dienstleistungen, welche von natürlichen Personen als Folge der zusätzlichen Transparenz einer Nachvollziehbarkeitslösung angefragt werden könnten, sind:

- Falls nicht bereits mit der Nachvollziehbarkeitslösung bereitgestellt: Was ist der Inhalt der gespeicherten Daten? Wie können fehlerhafte Daten korrigiert werden?
- Informationen zum «Recht auf Vergessen» oder dessen Durchsetzung: Wie lange darf die öffentliche Verwaltung einen Datensatz speichern und wie kann die Löschung überprüft und durchgesetzt werden?
- Natürliche Personen können gegenüber der öffentlichen Verwaltungen Stellvertretungen und Vollmachten definieren. Es wäre daher naheliegend zu fordern, auch Einsicht in diese zu erhalten.

6.12. Architektur & Schnittstellen

Sobald eine Nachvollziehbarkeitslösung umgesetzt werden soll, braucht es für eine Skalierung eine abgestimmte Systemarchitektur sowie dazugehörende Schnittstellen und Standards. Die Architektur muss im Hintergrund sicherstellen, dass die Anforderungen der natürlichen Personen erfüllt werden können und dass der Datenschutz und die Datensicherheit jederzeit gewährleistet sind. Bei der Wahl der Systemarchitektur sind insbesondere auch politische Rahmenbedingungen zu berücksichtigen: So wird eine stark zentralisierte Nachvollziehbarkeitslösung in der föderal organisierten Schweiz vermutlich auf wenig Akzeptanz stossen. Auch ein Datensammeln «auf Vorrat» wird kaum politische Mehrheiten finden. Die Architektur muss folglich eine Balance zwischen den verschiedenen Anforderungen finden. Weitere Details sind in Anhang A.11 aufgeführt.

6.13. Betrieb & Weiterentwicklung

Der Betrieb und die Weiterentwicklung der Nachvollziehbarkeitslösung müssen sichergestellt werden. Dieses Thema hängt jedoch stark von der gewählten Lösung und dem Vorgehen ab und wird daher in dieser Machbarkeitsstudie nicht weiter thematisiert. Das Thema ist im Rahmen der jeweiligen HERMES-Phasen eines allfälligen Umsetzungsprojektes zu adressieren.

6.14. Andere E-Gov Vorhaben, welche eine Umsetzung erleichtern können

Es gibt eine Vielzahl von anderen Vorhaben, welche die Umsetzung einer Nachvollziehbarkeitslösung vereinfachen können (siehe auch Anhang A.12). In der folgenden Liste sind exemplarisch einige ausgewählte Vorhaben aufgeführt:

Verwendung der AHVN13 in den Quellsystemen	Es ist mit den heutigen gesetzlichen Grundlagen möglich, die AVHN13 zu verwenden, um einen eindeutigen Identifikator für natürliche Personen zu haben[72]. Wird diese AHVN13-Nummer in den an die Nachvollziehbarkeitslösung anzuschliessenden Quellsystemen geführt, vereinfacht sich dadurch die Zuweisung von Daten zu einer natürlichen Person.
Verfügbarkeit einer nationalen E-ID	Eine national anerkannte E-ID vereinfacht die Authentifikation von natürlichen Personen gegenüber der Nachvollziehbarkeitslösung, indem eine zentrale Möglichkeit zur Authentifikation zur Verfügung gestellt wird.
Kantonale E-IDs	Auch kantonale E-IDs können als Möglichkeit zur Authentifikation verwendet werden.

[72] Siehe: https://www.zas.admin.ch/zas/de/home/partenaires-et-institutions-/navs13/utilisation-systematique-du-navs13.html

Kantonale / nationale Portale für nat. Personen	Vorhandene Portale können genutzt werden, um den natürlichen Personen Zugriff zu ihren Daten zu gewähren. Es braucht kein zusätzliches Zugangsportal für die Nachvollziehbarkeitslösung.
NaDB / IOP	Der Fortschritt bei der Standardisierung und Harmonisierung von Daten vereinfacht eine allfällige Aggregation von Daten aus verschiedenen Quellsystemen.
UZ14 Architektur	Eine übergeordnete Architektur kann Funktionalitäten einer Nachvollziehbarkeitslösung definieren.
UZ8 Stammdatenmanagement	Im Rahmen eines vereinheitlichten Stammdatenmanagements wird die Datenlandschaft der öffentlichen Verwaltung vereinfacht, was die Umsetzung einer Nachvollziehbarkeitslösung vereinfacht

7. Anwendungsfälle

7.1. Schlüsselerkenntnisse

Innerhalb des von UZ13 gesetzten Umfangs können **vier** verschiedene **Kategorien** von **Anwendungsfällen** unterschieden werden. Jede Kategorie dieser Anwendungsfälle stellt natürlichen Personen andere Informationen über ihre Personendaten und deren Verwendung zur Verfügung.

Anwendungsfälle der Kategorie «**Karte**» bieten natürlichen Personen **lediglich** einen **kleinen Mehrwert**, indem generisch aufgezeigt wird, in welchen Datensammlungen die eigenen Personendaten gespeichert sein könnten. Anwendungsfälle der Kategorie Karte weisen bereits beträchtlichen Komplexität für eine mögliche Umsetzung auf.

Anwendungsfälle der Kategorie «**Wer kennt mich?**» bieten natürlichen Personen einen **deutlichen Mehrwert** und wären verglichen mit den nachfolgenden umfangreicheren Varianten einfacher umsetzbar und auf viele Quellsysteme skalierbar. Als **unbeabsichtigter Nebeneffekt** könnte jedoch die **Anzahl** der **Auskunftsbegehren** gemäss Datenschutzgesetz von natürlichen Personen gegenüber der öffentlichen Verwaltung signifikant **ansteigen**, ohne dass dieser Prozess für die öffentliche Verwaltung vereinfacht wird.

Die Anwendungsfälle «**Self-Service Auskunft Datenschutzgesetz**» sowie «**Wer hat meine Daten genutzt?**» bieten natürlichen Personen insbesondere in Kombination einen grossen Mehrwert in Form von zusätzlicher Transparenz. Eine Umsetzung – insbesondere mit einer Vielzahl von Quellsystemen - ist komplex und aufwändig.

7.2. Übersicht über die Anwendungsfälle

Es wurden verschiedene Informationen identifiziert, welche natürlichen Personen im Rahmen der Nachvollziehbarkeitslösung zur Verfügung gestellt werden könnten (Tabelle 5 – linke Seite). Diese Informationen bedienen unterschiedliche Bedürfnisse der natürlichen Personen. Die Informationen wurden auf verschiedene Kategorien von Anwendungsfällen abgebildet (Tabelle 5 – oben). Es wird explizit von Kategorien von Anwendungsfällen gesprochen, da in jeder der Kategorien viele verschiedene Umsetzungen (Architektur, angeschlossene Quellsysteme, usw.) denkbar sind. Diese Kategorien von Anwendungsfällen sind im Folgenden kurz vorgestellt.

Tabelle 5: Übersicht über die bereitgestellten Informationen der präsentierten Anwendungsfälle

	«Karte»	«Wer kennt mich?»	«Self-Service Auskunft Datenschutzgesetz»	«Wer hat meine Daten genutzt?»
Verbesserte Darstellung rechtlicher Grundlagen	JA			
Auskunft darüber, in **welchen Quellsystemen** Daten über die betroffene Person vorhanden sind		JA	JA	JA
Auskunft darüber, **welche Daten** (inkl. Dateninhalt) in einem Quellsystem gespeichert sind			JA	optional
Auskunft darüber, **wann** und **durch wen** auf die persönlichen Daten **zugegriffen** wurde				JA
Auskunft darüber, **warum** auf die persönlichen Daten **zugegriffen** wurde				JA

7.3. Anwendungsfälle der Kategorie «Karte»

Die Anwendungsfälle der Kategorie «Karte» sollen natürlichen Personen aufzeigen, in welchen Quellsystemen der öffentlichen Verwaltung potenziell ihre Daten gespeichert sein können. Hierfür sollen öffentlich verfügbare Informationen verwendet werden. Geeignet als Datengrundlage wären beispielsweise die Register der Datenschutzbeauftragten von Bund und Kantonen sowie sämtliche Gesetze und Verordnungen auf allen Staatsebenen, welche die Erfassung und Verarbeitung von Daten regeln.

Abbildung 7 zeigt, wie eine solche «Karten»-Lösung aussehen könnte: Die natürliche Person gibt auf einer Website Informationen über sich sowie die Themen an, welche sie interessieren (linke Hälfte der Abbildung). Basierend auf den hinterlegten Informationen prüft die Website im Hintergrund, in welchen Quellsystemen potenziell Personendaten über die anfragende natürliche Person vorhanden sein könnten. Im einfachsten Fall wird als Resultat eine Liste der möglichen Quellsysteme angegeben (rechts oben in der Abbildung). Um die Nutzerfreundlichkeit zu erhöhen, könnten diese Resultate auch noch grafisch aufbereitet sowie durch bekannte Datenflüsse ergänzt werden (rechts unten in der Abbildung).

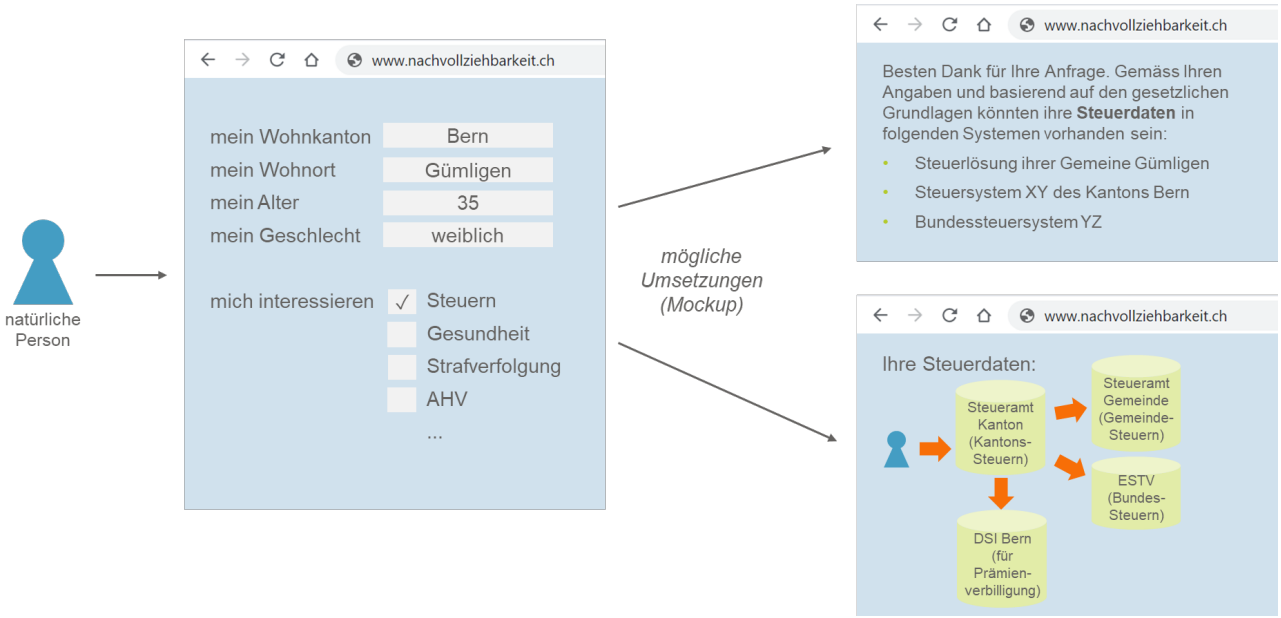

Abbildung 7: Mockup einer möglichen Umsetzung der Kategorie «Karte»

Wichtige Vorteile der Anwendungsfälle «Karte»:

- Aus technischer Sicht könnte sofort mit der Umsetzung angefangen werden.
- Aus gesetzgeberischer Sicht müsste lediglich einer oder mehreren Verwaltungsstellen der Auftrag erteilt werden, eine solche zentrale oder verteilte Lösung umzusetzen.
- Es braucht keine Anpassungen an bestehenden Quellsystemen.
- Die Lösung ist beliebig skalierbar.
- Es werden keine zusätzlichen Daten über natürliche Personen gesammelt.

Wichtige Nachteile der Anwendungsfälle «Karte»:

- Natürliche Personen erhalten keine Auskunft über zentrale Fragen der Nachvollziehbarkeit: In welchen Quellsystemen sind persönliche Daten über die natürliche Person tatsächlich gespeichert? Wann und durch wen wurde auf diese Personendaten zugegriffen? Was ist der Inhalt dieser Personendaten?

- Die Umsetzung sowie die Pflege der Datenbank dürften aufgrund der Komplexität der IT-Landschaft der öffentlichen Verwaltung einen grossen Aufwand erzeugen.

7.4. Anwendungsfälle der Kategorie «Wer kennt mich?»

Mit den Anwendungsfällen der Kategorie «Wer kennt mich?» soll natürlichen Personen explizit folgende Fragestellung beantwortet werden: «In welchen IT-Systemen der öffentlichen Verwaltung sind zum Stichtag X persönliche Daten über die betroffene natürliche Person gespeichert?». Hierzu müsste ein zentrales oder mehrere dezentrale (und ggf. föderierte) Nachvollziehbarkeitssysteme geschaffen werden, an welche angeschlossene Quellsysteme periodisch oder bei Bedarf melden, zu welchen natürlichen Personen Daten im betreffenden Quellsystem gespeichert sind.

Bei diesem Anwendungsfall ist es bereits zwingend notwendig, dass sich die natürliche Person gegenüber dem Nachvollziehbarkeitssystem identifiziert: Die Information darüber, ob in einem IT-System der öffentlichen Verwaltung Daten über eine natürliche Person gespeichert sind, lässt bereits Rückschlüsse über diese natürliche Person zu. So ist beispielsweise das Vorhandensein eines Datensatzes zu einer natürlichen Person in einem Betreibungsregister bereits als vertraulich zu klassifizieren und darf nicht ohne weiteres an Drittpersonen bekannt gegeben werden.

Der grösste Vorteil für natürliche Personen von Anwendungsfällen der Kategorie «Wer kennt mich» besteht darin, dass Transparenz hergestellt wird, in welchen Quellsystemen tatsächlich Personendaten über die natürliche Person gespeichert sind. Dies ermöglicht es natürlichen Personen bei Interesse gezielt bei den Eigentümern der betroffenen Quellsysteme ein Auskunftsbegehren gemäss Datenschutzgesetz zu stellen.

Eine mögliche Umsetzung von «Wer kennt mich?» ist in Abbildung 8 skizziert: Die verschiedenen Quellsysteme der öffentlichen Verwaltung (links im Bild) melden periodisch sämtliche AHVN13, zu welchen Datensätze gespeichert sind. Die in diesem Beispiel zentrale Nachvollziehbarkeitslösung sammelt diese Informationen (mittig im Bild). Die natürliche Person (rechts im Bild) identifiziert sich bei Interesse gegenüber der Nachvollziehbarkeitslösung und erhält eine Übersicht über sämtliche angeschlossenen Quellsysteme, in welchen die persönliche AHVN13 gespeichert ist.

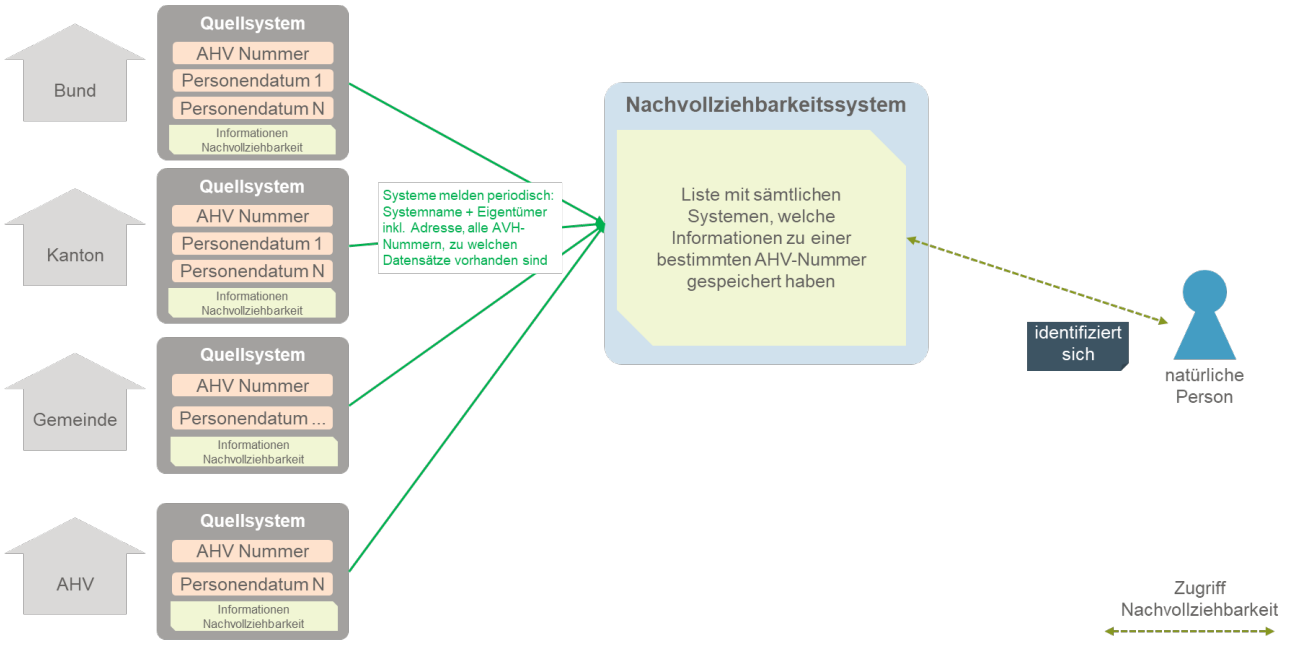

Abbildung 8: Eine mögliche Architektur zur Umsetzung von «Wer kennt mich?»

Wichtige Vorteile der Anwendungsfälle «Wer kennt mich»:

- Die technische Komplexität der Umsetzung ist verglichen mit den nachfolgenden Kategorien von Nachvollziehbarkeitslösungen geringer. Von technischer Seite her gibt es zwei zentrale Anforderungen:
    - Das Quellsystem muss Personendaten mit einem eindeutigen Identifikator (bspw. AHVN13) der natürlichen Person verbinden können.
    - Die natürliche Person muss sich mit einem ausreichenden Sicherheitslevel gegenüber der/den Nachvollziehbarkeitslösung identifizieren können.
- Gegenüber dem Status-Quo wird ein echter Mehrwert für natürliche Personen bezüglich der Transparenz zur Speicherung von Personendaten durch die öffentliche Verwaltung geschaffen.

Wichtige Nachteile von «Wer kennt mich»:

- Eine Lösung der Kategorie «Wer kennt mich» kann zu zusätzlichen Auskunftsbegehren gemäss Datenschutzgesetz führen, ohne jedoch diesen Prozess zu vereinfachen. Der Aufwand der betroffenen Verwaltungseinheiten zur Bearbeitung dieser Anfragen würde steigen.
- Eine Lösung der Kategorie «Wer kennt mich» liefert keine wirkliche Transparenz zur Frage, wie genau die Personendaten durch die Verwaltung genutzt werden.

7.5. Anwendungsfälle der Kategorie «Self-Service Auskunft Datenschutzgesetz»

Gemäss heute gängiger Praxis wird ein Auskunftsbegehren gemäss Datenschutzgesetz auf dem Korrespondenzweg per Post abgewickelt (siehe Abschnitt 5.2). Da natürliche Personen auch gegenüber privaten Unternehmen eine Auskunft gemäss Datenschutzgesetz verlangen können, haben gewisse private Unternehmen diesen Prozess bereits als «Self-Service» für natürliche Personen automatisiert. Eine natürliche Person, welche ein elektronisches «Kundenkonto» bei der entsprechenden Firma hat, kann die über sie gespeicherten Daten bei Bedarf einsehen und herunterladen.

Ein entsprechender Service könnte auch von Stellen der öffentlichen Verwaltung angeboten werden. Anstelle des «Kundenkontos» wäre in vielen Fällen die Identifikation der natürlichen Person mittels einer digitalen Identität sinnvoller[73], da oftmals kein entsprechendes «Kundenkonto» besteht. Eine solche Lösung könnte entweder zentral, teilweise zentral (bspw. pro Kanton) oder sogar komplett dezentral (pro Fachapplikation) angeboten werden.

Wichtige Vorteile der Anwendungsfälle «Self-Service Auskunft Datenschutzgesetz»:

- Der Aufwand der öffentlichen Verwaltung, um ein Auskunftsbegehren gemäss Datenschutzgesetz zu beantworten, wird signifikant reduziert oder sogar komplett vermieden. Die entsprechenden personellen Ressourcen können für andere Aufgaben verwendet werden.

Wichtige Nachteile der Anwendungsfälle «Self-Service Auskunft Datenschutzgesetz»:

- Eine Lösung der Kategorie «Wer kennt mich» liefert keine wirkliche Transparenz zur Frage, wie genau die Personendaten durch die Verwaltung genutzt werden. Es handelt sich lediglich um eine Digitalisierung des bestehenden Auskunftsprozesses.

[73] Gewisse Kantone haben eine solche bereits heute im Einsatz – beispielsweise das BE-Login, welches unter anderem für die Steuererklärung im Kanton Bern genutzt werden kann.

- Die Umsetzung dieser Anwendungsfälle ist komplex und aufwändig.

7.6. Anwendungsfälle der Kategorie «Wer hat meine Daten genutzt?»

Die Kategorie der Anwendungsfälle «Wer hat meine persönlichen Daten genutzt?» bietet natürlichen Personen den grössten Gewinn an Transparenz über die Verwendung der Personendaten durch die öffentliche Verwaltung. Die natürliche Person bekommt nicht nur Einsicht darüber, ob und gegebenenfalls welche Daten vorhanden sind, sondern auch, welche Verwaltungseinheit diese wann und zu welchem Zweck verwendet hat. Weitergehende Funktionalitäten wie Möglichkeit, explizit Zugriff auf Daten zu vergeben oder die Daten zu löschen sind gemäss Anhang A.2 nicht im Umfang dieser Machbarkeitsstudie[74].

Abbildung 9 skizziert eine Möglichkeit, wie ein Anwendungsfall der Kategorie «Wer hat meine Daten genutzt?» umgesetzt werden könnte: Die natürliche Person identifiziert sich gegenüber der zentralen[75] Nachvollziehbarkeitslösung (1). Es könnte der natürlichen Person von der Nachvollziehbarkeitslösung die Möglichkeit geboten werden, gewisse Themengebiete auszuwählen. Die Nachvollziehbarkeitslösung versendet[76] an sämtliche ausgewählten Quellsysteme eine Anfrage basierend auf der AHVN13 der natürlichen Person (2). Die angeschlossenen Quellsysteme stellen die Informationen zur Nachvollziehbarkeit basierend auf lokal gespeicherten Log-Dateien zusammen und senden diese zurück an die Nachvollziehbarkeitslösung (3). Optional könnten sogar die Inhalte der Personendaten mitgeliefert werden – in diesem Fall könnte diese Lösungsvariante auch die Informationen der Anwendungsfälle «Self-Service Auskunft Datenschutzgesetz» zur Verfügung stellen. Die Nachvollziehbarkeitslösung zeigt der natürlichen Person die Resultate der Anfrage bei den Quellsystemen an – entweder nach Quellsystem getrennt oder gegebenenfalls sogar nach Themengebiet aggregiert (4). Die so gesammelten Daten auf der Nachvollziehbarkeitslösung können im Anschluss zeitnah wieder gelöscht werden.

Für die Anwendungsfälle «Self-Service Auskunft Datenschutzgesetz» könnte grundsätzlich die gleiche Architektur verwendet werden – das Logging der Zugriffe auf Seite der Fachapplikationen würde allerdings entfallen.

---

[74] Es würde aus Sicht der natürlichen Personen möglicherweise ein Bedarf solcher Funktionalitäten bestehen. Solche Funktionalitäten wurden im elektronischen Patientendossier umgesetzt – siehe Abschnitt 5.6.2. Da erlaubte Zugriffe auf Daten sowie deren Speicherung oftmals auf Gesetzes- oder Verordnungsebene geregelt sind, ist eine solche Funktionalität im Sinne der Einschränkung meist nicht zielführend. Es könnte für natürliche Personen jedoch interessant sein, ihre Daten anderen Verwaltungseinheiten freizugeben, welche keinen gesetzlich geregelten Anspruch haben. Diese Funktionalität würde jedoch ausserhalb des Umfangs von UZ13 liegen und wird deshalb hier nicht weiter betrachtet.

[75] Selbstverständlich sind auch dezentrale oder föderierte Lösungen denkbar – um das Beispiel kurz zu halten, wurde in der Abbildung die konzeptionell einfachste Variante eines zentralen Nachvollziehbarkeitssystems gewählt.

[76] Hier sind beliebige Technologien möglich: API, Nachrichtenbus, …

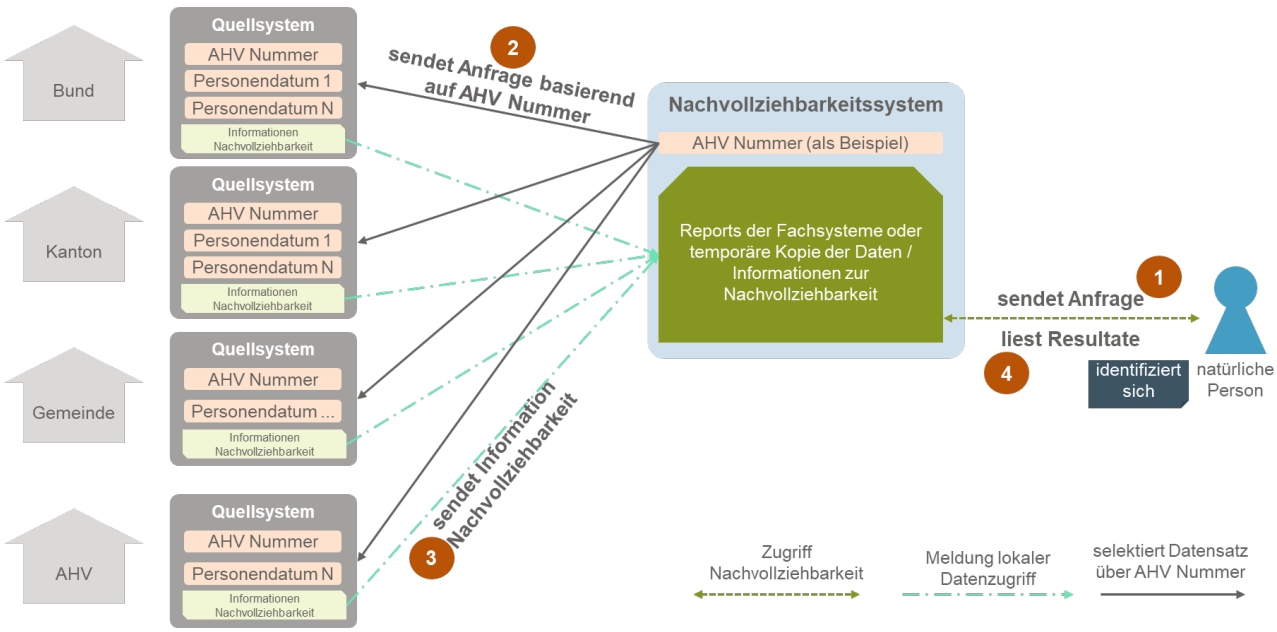

Abbildung 9: Eine mögliche (zentrale) Umsetzung von «Wer hat meine Daten genutzt?»

Wichtige Vorteile der Anwendungsfälle «Wer hat meine Daten genutzt?»:

- Diese Kategorie von Anwendungsfällen ermöglicht natürlichen Personen den grössten Transparenzgewinn aller vorgestellter Anwendungsfälle.

Wichtige Nachteile der Anwendungsfälle «Wer hat meine Daten genutzt»:

- Der Aufwand für die Umsetzung ist gross. Neben dem Aufbau einer oder mehrerer Nachvollziehbarkeitslösungen sind je nach Quellsystem umfangreichere Anpassungen notwendig.

8. Mögliche Varianten zur Fortführung von UZ13

8.1. Schlüsselerkenntnisse

Basierend auf dem in Kapitel 6 vorgestellten Lösungsraum und den in Kapitel 7 vorgestellten Anwendungsfällen wurden **Varianten** zur Fortführung von UZ13 **entworfen**. Diese Varianten **müssen umsetzbar** sein, **akzeptiert** werden und sie müssen einen **Schritt** in **Richtung** der **Vision** nach zusätzlicher Transparenz und Nachvollziehbarkeit für natürliche Personen im Bereich der Verwendung von Personendaten machen.

Als **Sofort-Massnahme** wird vorgeschlagen, die **kommunikativen Massnahmen** im Bereich der Verwendung von Personendaten zu verbessern.

Mittelfristig können mit einem **explorativen Vorgehen** in Form eines **Proof of Concepts** zusätzliche Erfahrungen anhand eines realen Anwendungsfalls gesammelt werden. Für die Umsetzung eines Proof of Concepts wurden **zwei Kategorien** von **Quellsystemen** als besonders interessant identifiziert: **Zentralisierte Datensammlungen** und **E-Government Portale der Kantone**. Um die Wahrscheinlichkeit für einen **Erfolg** bei der Umsetzung eines Proof of Concepts zu erhöhen, bietet sich ein **vorgelagerter** «**clickable Mockup**» an, um die natürlichen Personen ins Zentrum der Lösung zu stellen.

Diese Varianten werden durch die Varianten «Warten» und «andere transparenzsteigernde Vorhaben priorisiert umsetzen» ergänzt.

8.2. Die Eingrenzung des Lösungsraums in sinnvolle Optionen

Wie in Kapitel 6 aufgezeigt, besteht ein grosser Lösungsraum zur Umsetzung einer Nachvollziehbarkeitslösung. Die Schwierigkeit ist es, innerhalb von diesem Lösungsraum sinnvolle Varianten zu finden: Diese müssen umsetzbar sein, müssen das Ziel nach zusätzlicher Transparenz und Vertrauen für natürliche Personen erreichen und breit akzeptiert werden.

Für die Ausarbeitung von möglichen Varianten wird in diesem Kapitel auf die in Abbildung 10 farblich hervorgehobenen Themengebiete fokussiert: Die «Anwendungsfälle», die «Umsetzung» und die «anzuschliessenden Quellsysteme». Diese drei Themengebiete zeichnen sich durch zwei Charakteristika aus: Einerseits bestehen in diesen drei Themengebieten jeweils verschiedene Optionen, welche basierend auf dem heutigen Wissen bewertet werden können. Andererseits können basierend auf einer Variantenwahl in diesen drei Themengebieten Entscheide für die anderen Themengebiete abgeleitet werden[77] oder auf die Erfüllung von Anforderungen geprüft werden[78]. Basierend auf diesen drei Themengebieten werden im Rest von diesem Kapitel verschiedene Varianten für das weitere Vorgehen gebildet.

Nachdem ein Variantenentscheid gefällt wurde, können zu einem späteren Zeitpunkt Entscheide für andere Themengebiete wie beispielsweise die Architektur, den Betrieb oder notwendige Anpassungen an den rechtlichen Grundlagen abgeleitet werden. Jede Variante muss zudem die Anforderungen der natürlichen Personen und der Politik erfüllen. Diese Anforderungen können nur teilweise im Voraus definiert werden, da sie heute teilweise unbekannt sind und sich mit der Zeit ändern werden. Die Anforderungen müssen daher laufend neu evaluiert werden. Schlussendlich muss sich eine Lösungsvariante in die bestehende System-, Prozess- und Datenlandschaft einfügen. Allfällige notwendige Anpassungen müssen frühzeitig identifiziert und adressiert werden.

[77] Bspw. Betrieb und Weiterentwicklung, Daten, Prozesse & Leistungen

[78] Bspw. natürliche Personen & Bedürfnisse, Politik & Akzeptanz,

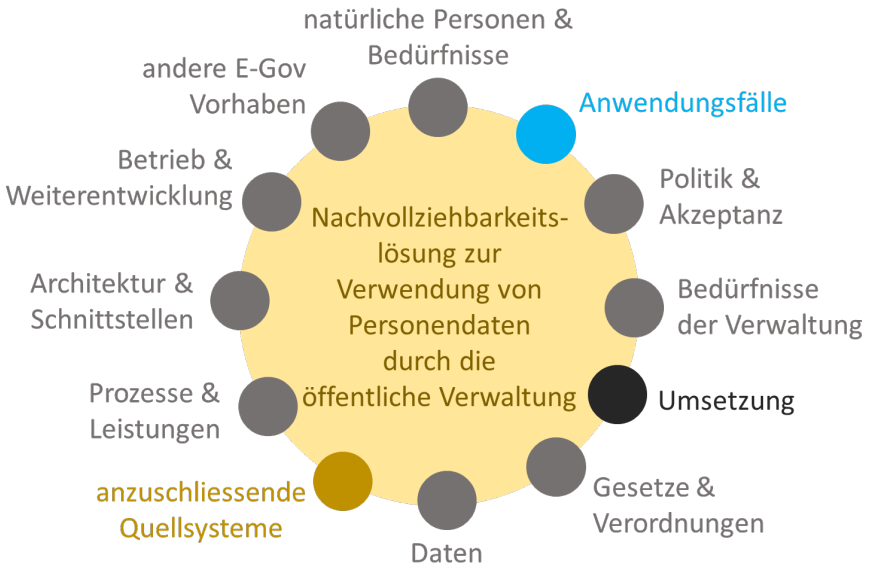

Abbildung 10: Themengebiete, basierend auf welchen verschiedene Varianten für das weitere Vorgehen gebildet werden.

8.3. Für Variantenbildung verwendete Anwendungsfälle

Im vorhergehenden Kapitel wurden vier mögliche Kategorien von Anwendungsfällen vorgestellt. Für die Variantenbildung wird auf die Anwendungsfälle der Kategorie «Wer hat meine Daten genutzt?» fokussiert, da diese gemäss aktueller Einschätzung den grössten Mehrwert liefern. Um natürlichen Personen zudem noch Einsicht in den Inhalt der Personendaten zu geben, können optional und ergänzend auch die Anwendungsfälle der Kategorie «Self-Service Auskunft Datenschutzgesetz» gleichzeitig umgesetzt werden. Die finale Entscheidung darüber, wie der konkrete Anwendungsfall (Kombination aus Quellsystem(en) und Granularität der angebotenen Informationen) im Detail aussieht, muss zu einem späteren Zeitpunkt getroffen werden.

Die anderen vorgestellten Kategorien von Anwendungsfällen bieten basierend auf dem heutigen Verständnis der Bedürfnisse von natürlichen Personen nicht ausreichend Mehrwert und werden für die Variantenbildung nicht berücksichtigt.

8.4. Für Variantenbildung verwendete Umsetzungsoptionen

Es gibt verschiedene Ansätze, wie eine Nachvollziehbarkeitslösung umgesetzt werden kann. Diese sind im Folgenden approximativ nach ansteigender Komplexität und Aufwand sortiert. Gewisse Umsetzungs-Ansätze können miteinander kombiniert werden.

Verbesserte Kommunikation als Sofort-Massnahme

Wie in Abschnitt 5.2 gezeigt, besteht in der Theorie durch die rechtlichen Grundlagen sowie die dazugehörenden Bereiche auf den Websites der Quellsysteme zum Thema «Datenschutz» bereits heute eine recht hohe Transparenz über die Verwendung der Personendaten durch die öffentliche Verwaltung. In der Praxis sind die typischerweise langen und in juristischer Sprache verfassten Texte für natürliche Personen schwer verständlich. Einfache und rasch umsetzbare Kommunikationsmassnahmen wie beispielsweise Infografiken können die Transparenz der Verwendung von Personendaten verbessern. Beispiele sind in Anhang A.14 aufgeführt.

Die Bedürfnisse der natürlichen Personen mittels «clickable Mockup» besser verstehen

Mit Hilfe von heutigen Technologien können auf eine schnelle Art und Weise Benutzeroberflächen von Programmen für Demonstrationszwecke erstellt werden, ohne dass dafür ein grosser finanzieller Aufwand notwendig ist. Solche simulierten Benutzeroberflächen ohne echte Funktionalität (hier «clickable Mockup» genannt) können dann natürlichen Personen präsentiert werden, damit diese das abstrakte Problem der Nachvollziehbarkeit der Verwendung von Personendaten aktiv erleben können. Die präsentierten Daten können fiktiv sein – müssen jedoch realitätsnah gewählt werden, um den testenden Personen ein möglichst authentisches Benutzererlebnis zu ermöglichen. Mit diesem Vorgehen sind keinerlei Anpassungen an den Quellsystemen notwendig und auch auf eine Authentifizierung kann verzichtet werden.

Um den grösstmöglichen Nutzen aus einem Mockup zu ziehen, wird dieser basierend auf dem Use-Case gemacht, welcher anschliessend umgesetzt werden soll. Der Mockup muss folglich in enger Zusammenarbeit mit dem oder den Partnern durchgeführt werden, welche für die an eine Nachvollziehbarkeitslösung anzuschliessenden Quellsysteme verantwortlich sind.

Die Verwendung eines Mockups erlaubt es ebenfalls, verschiedenen Lösungsvarianten miteinander zu vergleichen. Durch diesen relativ kostengünstigen Schritt kann geprüft werden, ob sich die Umsetzung eines Proof of Concepts lohnt und wie dieser ausgestaltet werden muss, damit dieser ein Erfolg wird.

Als Grundlage für einen Mockup können auch die Ergebnisse der E-Government Umfrage 2021 weitere Einsichten liefern.

Erfahrung sammeln durch Umsetzung eines Proof of Concepts

Die Nachvollziehbarkeitslösung wird anhand von einem «Proof of Concept» umgesetzt. Ein Proof of Concept kann entweder isoliert mit einem einzigen Quellsystem oder mit einer kleinen Anzahl von Quellsystemen umgesetzt werden. Idealerweise wird der Proof of Concept so gewählt, dass damit ein möglichst klar definierter aktueller Bedarf von natürlichen Personen umgesetzt werden kann. Um die Chancen auf eine erfolgreiche Umsetzung zu erhöhen, kann ein Proof of Concept mit einem Mockup verbunden werden. Mögliche Fragestellungen, welche im Rahmen eines Proof of Concepts geklärt werden können, sind in Anhang A.15 aufgeführt.

Nicht weiter betrachtet wird vorderhand eine Nachvollziehbarkeitslösung mit vielen angeschlossenen Quellsystemen, da aktuell viele Voraussetzungen fehlen: Ein detailliertes Verständnis der Anforderungen der natürlichen Personen, diverse «Enabler» als auch Erfahrungen und ein politischer Auftrag. Zu einem späteren Zeitpunkt nach einer allfälligen erfolgreichen Umsetzung eines Proof of Concepts kann nochmals geprüft werden, ob eine Skalierung der Nachvollziehbarkeitslösung durch Anschluss weiterer Quellsysteme zielführend ist.

Zusammengefasst werden sowohl die Sofort-Massnahme der verbesserten Kommunikation als auch ein exploratives Vorgehen mit einer Kombination eines Proof of Concepts und vorgelagertem Mockup empfohlen.

8.5. Für Variantenbildung verwendete Quellsysteme

Basierend auf der Empfehlung, einen «Proof of Concept» mit einem oder wenigen Quellsystemen durchzuführen, reduzieren sich die Optionen zur Anbindung von Quellsystemen markant[79]: Es müssen ein oder mehrere Systeme identifiziert werden, welche sich für einen Proof of Concept eignen. Im Rahmen der Machbarkeitsstudie wurden exemplarisch mögliche Opportunitäten für die Umsetzung eines «Proof of Concepts» identifiziert. Die Opportunitäten zeichnen sich dadurch aus[80], dass für natürliche Personen jeweils eine klare «Storyline» vorhanden ist, weshalb der Proof of Concept konkret zu mehr Transparenz führt.

Zentralisierte Quellsysteme

Gewisse Quellsysteme sind bereits zentralisiert aufgebaut (bspw. Personenstandregister Infostar) oder wurden/werden zentralisiert (bspw. Nationaler Adressdienst). Durch die Zentralisierung wandern die Daten von den Gemeinden / Kantonen zum Bund. Für natürliche Personen kann dies so aussehen, als ob dadurch mehr Stellen der öffentlichen Verwaltung auf die entsprechende Information zugreifen können, als dies früher der Fall war. Als Gegenmassnahme könnte die Nachvollziehbarkeitslösung hier Transparenz über die erfolgten Zugriffe und deren Gründe liefern.

Ein **Spezialfall** eines zentralisierten Quellsystems ist das **UPI-Register**, in welchem die AHVN13 Nummer gespeichert ist. Mit der neu erlaubten systematischen Verwendung der AHVN13 wird diese vermutlich in vielen Systemen gespeichert und regelmässig abgeglichen werden. Eine Nachvollziehbarkeitslösung basierend auf dem UPI-Register würde einer natürlichen Person neben der Information bezüglich des Zugriffs auf die Daten auch eine recht gute Übersicht über die Systeme liefern, in welchen Personendaten über sie gespeichert sind.

Ein weiterer **Spezialfall** ist der **Nationale Adressdienst (NAD)**: Das entsprechende System befindet sich aktuell erst im Aufbau. Gemäss aktuellem Gesetzesentwurf zum NAD wird das System gewisse Funktionalitäten implementieren, um das Auskunftsrecht zu gewährleisten.

Ein kantonales E-Government-Portal

Die Verwendung eines kantonalen E-Government-Portals (siehe auch Anhang A.4) für einen Proof of Concept hat den Vorteil, dass bereits Schnittstellen zwischen dem Portal und den Fachanwendungen bestehen. Zudem ist mit dem Portal auch eine Benutzeroberfläche und ein Login vorhanden. Neben der Bereitstellung zusätzlicher Transparenz für natürliche Personen könnte in einem solchen Setting auch das Auskunftsbegehren gemäss Datenschutzgesetz über die Plattform für die angeschlossenen Quellsysteme abgewickelt werden, was die entsprechenden Verwaltungsstellen entlasten würde.

---

[79] Bei der Einführung einer Nachvollziehbarkeitslösung mit vielen angeschlossenen Quellsystemen ergeben sich weitere Optionen:
- Den Entscheid über die Anbindung des Quellsystems dessen Eigentümer überlassen
- Die Anbindung bei Ersatz des Quellsystems verbindlich erklären
- Analog zu Estland eine Anzahl Systeme definieren, welche als wichtig erachtet werden oder Systeme entlang einem priorisierten Backlog einbinden.

[80] Weitere mögliche Kriterien für die Auswahl von Systemen sind (Liste nicht abschliessend): Anzahl der natürlichen Personen, von welchen im Quellsystem Informationen gespeichert sind; Besonders sensitive Bereiche (bspw. Gesundheit, Migration, Recht & Polizei) oder vulnerable Personen (bspw. IV / Kinder / Asylbereich / Sozialhilfe / Altenpflege); Vorhandensein von besonders schützenswerten Personendaten; Quellsysteme, auf welchen viele Zugriffe und Änderungen stattfinden; Anzahl von Organisationseinheiten, welche auf das System Zugriff haben; Aktuelle politische Relevanz des Systems; Ist eine Ablösung des Quellsystems geplant?; Einfachheit der Anbindung des Quellsystems; Quellsysteme, welche entlang der Prozesskette von für natürlichen Personen besonders wichtigen Prozessen sind.

Möglichst einfaches Quellsystem

Die Umsetzung eines Proof of Concepts wird erschwert, wenn das oder die Quellsysteme eine hohe Komplexität aufweisen. Alternativ zu den vorhergehenden Vorschlägen kann nach möglichst einfachen Quellsystemen (bspw. auch auf Stufe Kanton oder Gemeinde) gesucht werden, um einen Proof of Concept umzusetzen. Dabei ist darauf zu achten, dass die Umsetzung der Nachvollziehbarkeit der Verwendung von Personendaten im betreffenden System für eine ausreichend grosse Anzahl von natürlichen Personen von Interesse ist. Auch ist darauf zu achten, dass auf dem Quellsystem regelmässige Zugriffe stattfinden. Ist dies nicht der Fall, so kann mit dem Proof of Concept für natürliche Personen kein Mehrwert geschaffen werden und folglich wird es auch nur begrenzt möglich sein, mehr über die Bedürfnisse der natürlichen Personen zu lernen.

8.6. Mögliche Varianten zur Fortführung von UZ13

Kombiniert ergeben sich somit folgende möglichen Varianten zur Fortsetzung von UZ13:

Verbesserte Kommunikation als Sofort-Massnahme

Die Kommunikation darüber, welche Personendaten zu welchem Zweck in einem IT-System einer öffentlichen Verwaltung geführt werden, kann in vielen Fällen optimiert werden. Es bieten sich beispielsweise Infografiken oder auch Erklärvideos an. Zur Unterstützung dieser Massnahmen können Beispiele, Vorlagen oder Guidelines erarbeitet werden.

Clickable Mockup auf Basis eines möglichen Proof of Concepts

Ein Mockup basierend auf einem konkreten Anwendungsfall und in enger Zusammenarbeit mit einem oder mehreren möglichen Partnern für einen Proof of Concept erstellen. Der Mock-Up kann mit natürlichen Personen getestet werden, um daraus abgeleitet den Umfang und die Funktionalitäten eines Proof of Concepts (POC) zu schärfen.

Proof of Concept mit einem zentralen Quellsystem

Mögliche Beispiele für einen Proof of Concept mit einem zentralisierten Quellsystem sind: Infostar, der Nationale Adressdienst (NAD), das Fahrzeughalterregister des ASTRA oder auch das UPI-Register. Die für natürliche Personen bereitgestellten Informationen sollen Antworten auf die Fragen geben, welche Daten vorhanden sind, und wer zu welchem Zeitpunkt mit welcher Begründung auf die Daten zugegriffen hat (Kombination der Anwendungsfälle «Self-Service Auskunft Datenschutzgesetz» und «Wer hat meine Daten genutzt?»). Die je nach Quellsystem bereits hohe Komplexität ist bei der Auswahl des Proof of Concepts zu berücksichtigen.

Proof of Concept mit mehreren zentralen Quellsystemen

Analog zur obenstehenden Variante, jedoch sollen an die Nachvollziehbarkeitslösung nicht nur eines, sondern mehrere Quellsysteme angebunden werden.

Proof of Concept mit einem kantonalen Portal

Analog zu den obenstehenden Varianten, jedoch wird der Proof of Concept mit einem kantonalen E-Government Portal[81] sowie ausgewählten oder allen angeschlossenen Quellsystemen durchgeführt.

Proof of Concept mit einem möglichst einfachen Quellsystem

Analog zu den obenstehenden Varianten, jedoch wird für den Proof of Concept ein möglichst einfaches und gleichzeitig für natürliche Personen dennoch relevantes Quellsystem gewählt.

Es werden zudem folgende zwei generischen Varianten ergänzt:

[81] Mit dem Verein iGovPortal.ch wurde exemplarisch ein erstes Sondierungsgespräch geführt, bei welchem grundsätzliches Interesse bekundet wurde. Im Verein iGovPortal.ch sind die Kantone Freiburg, Graubünden, Jura, St.Gallen und Solothurn vertreten. Sämtliche anderen kantonalen E-Government Portale (siehe auch Anhang A.4) wären weitere Kandidaten für einen Proof of Concept.

Warten	Diverse Enabler fehlen aktuell (siehe auch Abschnitt 5.5.2). Es soll mit der Fortsetzung von UZ13 gewartet werden, bis diese Enabler vorhanden sind.
Andere Massnahmen	Es gibt neben den in UZ13 skizzierten Lösungsvarianten viele weitere Massnahmen zur Transparenzsteigerung, welche alternativ umgesetzt werden könnten. Der EU-Benchmark (siehe Abschnitt 4.3) liefert hierzu mögliche Ansatzpunkte.

9. Bewertung der Varianten zur Fortführung von UZ13

Die erarbeiteten Varianten werden in Abbildung 11 basierend auf verschiedenen Kriterien qualitativ bewertet. Die Varianten sind in der linken Spalte aufgeführt, die Bewertungskriterien in der ersten Zeile. Die qualitative Bewertung der Lösungsvarianten findet sich in der letzten Spalte. Grün bedeutet eine positive Bewertung, gelb eine neutrale und rot eine negative Bewertung.

Die Umsetzung von Kommunikationsmassnahmen wird grundsätzlich positiv bewertet. Auch die Umsetzung eines «clickable Mockups» wird positiv bewertet. Dabei ist jedoch zu beachten, dass dieser nur in Kombination mit einem möglichen Proof of Concept den vollen Nutzen entfalten kann.

Die verschiedenen Varianten der Umsetzung eines Proof of Concepts werden generell als zielführend betrachtet, jedoch sind diverse Abhängigkeiten zu fehlenden Enablern vorhanden, welche eine sofortige Umsetzung erschweren. Die Umsetzung eines Proof of Concepts mit verschiedenen zentralisierten Quellsystemen hat die grössten Abhängigkeiten mit noch nicht vorhandenen Enablern.

Reines «warten auf bessere Zeiten» bringt das Thema der Nachvollziehbarkeit der Verwendung von Personendaten nicht vorwärts und wird daher negativ bewertet. Die Umsetzung alternativer Massnahmen zur Förderung von Transparenz ausserhalb des Scopes von UZ13 kann zielführend sein, falls diese Massnahmen verglichen mit einer Nachvollziehbarkeitslösung mehr Transparenz und Vertrauen schaffen können.

	Bedarf besser verstehen	Erwarteter Nutzen für natürliche Personen	Aufwand / Komplexität	Involvierte Partner	Abhängigkeiten zu «Enablern» (E-ID, Portale)	Dauer erfolgreiche Umsetzung	Chancen auf erfolgreiche Umsetzung	**Bewertung**
Verbesserte Kommunikation	*Gering, ev. indirekt über Feedback*	*Hoch*	*Gering-Mittel*	*Möglichst viele*	*Keine*	*Schnell umsetzbar, wenn Partner mitmachen*	*Hoch, falls Partner mitmachen*	Unabhängig von anderen Varianten umsetzen
Clickable Mockup	*Hoch*	*Nur in Kombination mit anschliessendem Proof of Concept*	*Gering-Mittel*	*Idealerweise sind bereits mögliche Partner für POC bekannt*	*Keine*	*Schnell umsetzbar*	*Hoch, Schwierigkeit wird sein, passende Partner für anschliessenden POC zu finden*	Kann gestartet werden, sobald mögliche Partner für einen POC vorhanden sind
Proof of Concept (POC) mit zentralem Quellsystem	*Mittel*	*Mittel bis Hoch*	*Mittel*	*Ein geeigneter Partner*	*E-ID, Portal zur Anzeige*	*Mittelfristig (Abhängigkeiten)*	*Mittel – offene Fragen bezüglich E-ID; gegebenenfalls Möglichkeit, bestehende E-IDs der Kantone zu nutzen*	Da eine nationale E-ID fehlt, müssen alternative Lösungsansätze gesucht werden – beispielsweise über die Einbindung in ein kantonales Portal (siehe auch Lösung POC kantonales Portal)
Proof of Concept mit mehreren zentralen Quellsystemen	*Mittel*	*Hoch*	*Hoch*	*Mehrere geeignete Partner*	*E-ID, Portal zur Anzeige, Standardisierung und Harmonisierung von Daten*	*Mittelfristig (Abhängigkeiten)*	*Mittel, siehe Variante oben: Zusätzliche Schwierigkeit von zusätzlichen Partnern*	Als Ausbaustufe zum POC mit einem Quellsystem (obere Zeile) als zweiter Schritt
Proof of Concept mit einem kantonalen Portal	*Mittel*	*Hoch*	*Hoch*	*Sämtliche am Portal beteiligten Partner*	*Standardisierung und Harmonisierung von Daten*	*Mittelfristig (geeignete Partner notwendig)*	*Mittel, da recht hohe Komplexität aufgrund von vielen Partnern*	Grundsätzlich mit einem Partner zusammen umsetzbar – es bestehen jedoch offene Fragen im Bereich der Datenhaltung
Proof of Concept mit einfachem dezentralen Quellsystem	*Gering-Mittel*	*Gering-Mittel*	*Gering-Mittel*	*Ein geeigneter Partner*	*E-ID, Portal zur Anzeige*	*Mittelfristig (Abhängigkeiten)*	*Hoch-Mittel (geringere Komplexität Quellsystem, Abhängigkeiten bestehen)*	Macht dann Sinn, wenn ein Quellsystem gefunden werden kann, welches eine geringe Komplexität aufweist und für natürliche Personen einen Mehrwert bietet
Warten	*Nur mit zusätzlichen Begleitmassnahmen*	*Kein Nutzen*	*Gering*	*Keine*	*E-ID, Portal zur Anzeige, ...*	*Lange*	*Unklar ob Warten die Chancen erhöht oder senkt*	Nicht empfohlen
Andere Massnahmen	*Je nach Massnahme*							Potenzieller Nutzen von UZ13 mit Nutzen von anderen Transparenzvorhaben zu vergleichen

Abbildung 11: Bewertung der verschiedenen Lösungsvarianten.

10. Empfehlungen weiteres Vorgehen durch Fachausschuss

Zum heutigen Zeitpunkt ist die Umsetzung einer Nachvollziehbarkeitslösung mit vielen angeschlossenen Quellsystemen nicht zielführend. Die folgenden Empfehlungen ermöglichen es, das Thema der Nachvollziehbarkeit weiterhin aktiv weiterzuverfolgen und Schritte in die Richtung der Vision von zusätzlicher Transparenz und Nachvollziehbarkeit für natürliche Personen zu machen.

Der Fachausschuss von UZ13 empfiehlt, das Thema der Nachvollziehbarkeit der Verwendung von Personendaten durch die öffentliche Verwaltung im Rahmen der «Agenda DVS[82]» weiterzuverfolgen. Folgende vier Punkte werden zur Umsetzung empfohlen:

Partner für einen möglichen Proof of Concept evaluieren	Um einen Mockup und anschliessend basierend auf dem gleichen Use-Case einen Proof of Concept umzusetzen, müssen geeignete Partner gefunden werden. Mit diesem oder diesen Partnern soll verifiziert werden, ob und wie ein Proof of Concept von einer Nachvollziehbarkeitslösung umgesetzt werden könnte. Mit dem vorgeschlagenen explorativen Vorgehen können mit begrenztem Aufwand und Risiko die Bedürfnisse und Anforderungen von natürlichen Personen im Zusammenhang mit der Nachvollziehbarkeit der Verwendung von Personendaten durch die öffentliche Verwaltung präzisiert werden. Weiter ermöglicht die Umsetzung eines Proof of Concepts natürlichen Personen zusätzliche Transparenz über die Verwendung von Personendaten – wenn auch in einem begrenzten Umfang.
Arbeit an Enablern fortsetzen	Wichtige Enabler (E-ID, nationales Datenmanagement, Harmonisierung und Standardisierung von Daten, Verwendung eindeutiger und übergreifender Identifikatoren) sind zu etablieren, da diese die Grundlage für eine mögliche skalierbare «Nachvollziehbarkeitslösung» darstellen. Diese Enabler werden zudem auch für andere E-Government Vorhaben wichtig sein.
Kommunikative Massnahmen zur Verbesserung der Transparenz umsetzen	Es wird empfohlen, zusätzliche kommunikative Massnahmen zur Förderung von Transparenz bei der Verwendung von Personendaten bei natürlichen Personen umzusetzen. Mögliche Massnahmen sind die Erstellung von Infografiken oder auch Erklärvideos für einzelne Systeme. Ein Pilot mit einem oder wenigen ausgewählten zentralisierten Registern kann genutzt werden, um gemeinsam mit Nutzergruppen geeignete Kommunikationsmassnahmen zu definieren. Um die verschiedenen Systembetreibenden dabei zu unterstützen, solche kommunikativen Massnahmen umzusetzen, sollen Beispiele, Best Practices oder Vorlagen etabliert werden. Diese Kommunikationsmassnahmen können zusätzlich auch zentral gesammelt werden – ch.ch würde sich dafür beispielsweise anbieten. Bei neu geschaffenen oder überarbeiteten Dienstleistungen («Services») der öffentlichen Verwaltung soll eine verbesserte Kommunikation sowie die Möglichkeit zur Einsicht in die Verwendung von Personendaten bereits bei der Konzeption berücksichtigt werden.

[82] DVS = Digitale Verwaltung Schweiz
https://www.efd.admin.ch/efd/de/home/digitalisierung/e-government-schweiz.html
https://www.newsd.admin.ch/newsd/message/attachments/67071.pdf

Das Thema der Nachvollziehbarkeit der Verwendung von Personendaten weiterverfolgen und in bestehenden Organisationen verankern

Es ist davon auszugehen, dass das Thema der Transparenz der Verwendung von Personendaten in Zukunft ein steigendes Interesse erfahren wird. Die Auskunft zur Verwendung der Personendaten ist im elektronischen Patientendossier umgesetzt und im Gesetzesentwurf zum Nationalen Adressdienst ebenfalls vorgesehen[83]. Mit dieser Machbarkeitsstudie wurde ein Schritt in Richtung einer Nachvollziehbarkeitslösung gemacht. Um das Thema aktiv weiterzuverfolgen, wird empfohlen, dieses im Rahmen der «Agenda DVS» weiterzuverfolgen. Die Studie soll publiziert und bei den relevanten Stakeholdern vorgestellt werden, sodass diese bei Interesse aktiv in die Weiterverfolgung eingebunden werden können. Folgende nicht abschliessende Liste zeigt mögliche relevante Stakeholder:

- eCH (Standardisierung von Services)
- Bundeskanzlei (als Betreiber von ch.ch)
- EDÖB (Eidgenössischer Öffentlichkeits- und Datenschutzbeauftragter)
- BK DTI (Digitale Transformation und IKT-Lenkung)
- Netzwerk Digitale Selbstbestimmung
- bei den Portalbetreibern (Bund und Kantone), welche ein wichtiger Kontaktpunkt zu den natürlichen Personen sind
- im Umsetzungsziel 14 «Architektur»
- bei den grösseren Registern (NAD, UPI, INFOSTAR, ...)

[83] https://www.newsd.admin.ch/newsd/message/attachments/57988.pdf Artikel 10 «Protokollierung und Auskunftsrecht der betroffenen Person»

A. Anhang

A.1. Vorgehen zur Erarbeitung der Machbarkeitsstudie

Bei Projektbeginn hat sich herausgestellt, dass das ursprüngliche Ziel

> *«eines Konzepts für die Architektur eines Logsystems, das der Bevölkerung aufzeigt, welche persönlichen Daten eine Behörde eingesehen oder genutzt hat»*

aufgrund des extrem umfangreichen Lösungsraumes nicht ohne weiteres möglich ist. Das Umsetzungsziel wurde darauf basierend angepasst:

> *«Machbarkeitsstudie zur Nachvollziehbarkeit der Verwendung persönlicher Daten erarbeiten»*

Das Projekt agiert folglich in der Initialisierungs-Phase von HERMES. Auf die Erstellung eines Projektauftrags sowie eines Projektmanagementplanes wurde vorderhand verzichtet, da nicht klar war, ob bei Abschluss der Machbarkeitsstudie ein Projekt beauftragt würde.

In der ersten Phase des Projekts wurde der Projektumfang gemeinsam mit dem Auftraggeber und dem Fachausschuss erarbeitet. Hierfür wurde ein morphologischer Kasten erstellt. Die daraus entstandene «Grobanalyse» ist in Anhang A.2 aufgeführt. Dieser Projektumfang wurde im Rahmen der Machbarkeitsstudie punktuell weiter präzisiert.

Die vorliegende Machbarkeitsstudie wurde durch die Autoren der AWK Group verfasst. Zwischenresultate wurden regelmässig mit dem Fachausschuss besprochen und durch diesen ergänzt (insgesamt 5 halbtätige Workshops). Punktuell wurden weitere Gespräche mit einzelnen Mitgliedern des Fachausschusses sowie weiteren Personen zur Vertiefung von einzelnen Themen geführt. Der Auftraggeber wurde regelmässig über Zwischenresultate informiert und konnte zu diesen Stellung nehmen. Die finale Version der Machbarkeitsstudie wurde den Mitgliedern des Fachausschusses zum Review vorgelegt.

Die Projektorganisation sowie weitere Eckpunkte sind im folgenden Projekt-Steckbrief aufgeführt.

Projektdauer	August 2020 – Dezember 2021
Projektauftrag basierend auf	Umsetzungsziel 13 des Umsetzungsplans E-Government 2021-2023 der E-Government-Strategie Schweiz 2020–2023. https://www.egovernment.ch/de/umsetzung/umsetzungsplan/
Auftraggeber	Peppino Giarritta, Auftraggeber (DVS / Digitale Verwaltung Schweiz, ab April 2021) Cédric Roy, Auftraggeber (E-Government Schweiz, bis April 2021) Marcel Kessler, Projektleiter (E-Government Schweiz, ehemals ISB)
Projektteam AWK Group AG	Dominik Bischoff (AWK Group AG) Andreas Meier (AWK Group AG) Alexander Zurkinden (AWK Group AG, bis Januar 2021)
Fachausschuss	Marianne Fraefel - Projektleiterin UZ10, Nationaler Adressdienst - BFS Hansjörg Hänggi - Leiter Digitalisierung & Innovation Kanton - BS Andreas Spichiger - Leiter Architektur - DTI Thomas Steimer - Umsetzungsprojektmanager E-Government - BJ Dieter Tschan - E-Government-Koordinator des Bundes - BK Jürg Wüst - Projektleiter UZ14, Architektur - DTI Andrin Eichin - Policy Advisor - BAKOM Thomas Schneider - Netzwerk digitale Selbstbestimmung - BAKOM Roger Dubach - Netzwerk digitale Selbstbestimmung - EDA Irem Kaynarca - Projektleiterin Monitoring – DVS Schweiz, ehemals ISB

A.2. Grobanalyse

Dieses Kapitel behandelt den möglichen Umfang einer Nachvollziehbarkeitslösung und steckt damit auch den Raum an Aspekten ab, welche im Rahmen der Erarbeitung der Lösungsvarianten berücksichtigen werden. Der gesamtheitliche Umfang wurde dabei in sieben Themengebiete unterteilt, siehe Tabelle 1, wobei jedes dieser Gebiete in einem separaten Abschnitt dieses Kapitels behandelt wird. Je Gebiet wurden die relevanten Themen identifiziert und deren möglichen Ausprägungen in «in Scope» und «out-of Scope» unterteilt. Wobei diese Unterteilung folgende Bedeutung hat:

- *«In Scope»* Ausprägung soll zur Abdeckung des Bedarfs bei der Variantenwahl berücksichtigt werden
- *«Out-of Scope»* Ausprägung welche bei der Ausarbeitung der Lösungsvarianten bewusst nicht berücksichtigt werden soll

A.2.1. Nutzende der Nachvollziehbarkeitslösung

Teil dieses Themengebiets ist das Thema «Personen, welche von einer Nachvollziehbarkeitslösung profitieren sollen». Die Abbildung 12 zeigt die Details dieses Themengebiets auf.

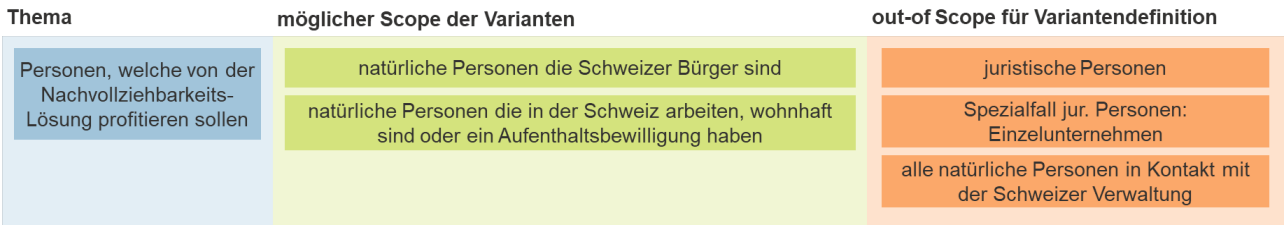

Abbildung 12: Übersicht der Themen des Themengebiets «Nutzende der Nachvollziehbarkeitslösung»

Als mögliche Nutzende einer Nachvollziehbarkeitslösung kommen grundsätzlich zwei Gruppen in Frage: natürlichen Personen und juristischen Personen.

Es wurde entschieden, sich in UZ13 auf die natürlichen Personen zu fokussieren, da bei diesen ein grösserer Bedarf an Nachvollziehbarkeit der Datennutzung durch die Verwaltung erwartet wird. Juristische Personen wurden bewusst als out-of Scope definiert. Ihre Bedürfnisse werden in separaten UZ, unter anderem UZ1 EasyGov.swiss, adressiert.

Es wurde die Hypothese gewählt, wonach jede natürliche Person, welche regelmässig im Kontakt mit der Schweizer Verwaltung ist, von der Nachvollziehbarkeitslösung potentiell profitieren können soll. Dies sind:

- natürliche Personen die Schweizer Bürger sind
- natürliche Personen, welche in der Schweiz wohnhaft sind oder in der Schweiz arbeiten
- natürliche Personen, welche in der Schweiz eine Aufenthaltsbewilligung (bspw. Flüchtlingsstatus) haben

Explizit ausgeschlossen werden Personen, welche nur vereinzelten und flüchtigen Kontakt mit der Verwaltung in der Schweiz haben (beispielsweise in der Schweiz im Urlaub oder auf der Durchreise sind). Von solchen natürlichen Personen dürften im Allgemeinen keine oder nur wenige Perso-

nendaten in den Systemen der Schweizer Verwaltung vorhanden sein. Zudem kann eine eindeutige Identifizierung solcher natürlichen Personen schwierig sein.

A.2.2. Auskunft über Daten, Verwendung und Weitergabe

Das Themengebiet «Auskunft über Daten, Verwendung und Weitergabe» ist in fünf Themen gegliedert. Abbildung 13 zeigt die Details dieses Themengebiets auf.

Thema	möglicher Scope der Varianten	out-of Scope für Variantendefinition
Welche Information zur Daten Verwendung werden dem Nutzenden geben*	Daten wurden genutzt	Keine Aussage über Verwendung
	Daten wurden weitergegeben	Weitergabe-Berechtigung
	Daten sind vorhanden	Verwendungs-Berechtigung
	Historischer Verlauf (Erhebung / Anpassung / Löschung)	Aggregierte / anonymisierte Daten
Details zur Nutzung	Nutzung durch Stelle S** (durch wen)	
	Nutzung für Prozess P** (Zweck)	
	Nutzung für Leistung L** (Zweck)	
	Nutzung basierend auf Rechtsgrundlage R** (worauf basierend)	
Details zur Datenweitergabe (verwaltungsintern, wie - extern)	Verwaltungseinheit hat Personendaten von Person X von Organisation O bekommen	Verwaltungseinheit darf Personendaten von Organisation O entgegen nehmen
	Verwaltungseinheit hat Personendaten von Person X an Organisation O weitergeben	Verwaltungseinheit darf Personendaten vom Typ Y von Organisation O entgegen nehmen
	Verwaltungseinheit hat Personendaten von Person X vom Typ Y*** an Organisation O weitergeben	Verwaltungseinheit darf Personendaten vom Typ Y an Organisation O weitergeben
	Verwaltungseinheit hat Personendaten von Person X vom Typ Y*** von Organisation O bekommen	Verwaltungseinheit darf Personendaten an Organisation O weitergeben
	Weitergabe basierend auf Prozess / Leistung (nicht zwingend von Bürger abgerufen)	Verwaltungseinheit hat Personendaten von Person X vom Typ Y mit Inhalt I an Organisation O weitergeben
		Verwaltungseinheit hat Personendaten von Person X vom Typ Y mit Inhalt I von Organisation O bekommen
		Weitergabe basierend auf Rechtsgrundlage (weniger wichtig als Leistung)
Details zu gespeicherten Daten	Personendaten von Person X gespeichert: Ja / Nein	Verwaltungseinheit darf Personendaten vom Typ Y erfassen (entspricht in etwa Status-Quo)
	Personendaten von Person X vom Typ Y gespeichert	
	Personendaten von Person X vom Typ Y mit Metadaten M gespeichert	
	Personendaten von Person X vom Typ Y mit Inhalt Z (und Metadaten M) gespeichert****	
historischer Verlauf (wann)	Nachvollziehbarkeits-Lösung gibt Auskunft über heutigen Datenbestand	Nachvollziehbarkeits-Lösung zeigt Historie der Daten auf (Dateninhalt)
	Nachvollziehbarkeits-Lösung zeigt Historie der Zugriffe auf	
	Nachvollziehbarkeits-Lösung zeigt Historie der Datenweitergaben auf	
	Historischer Verlauf des Lifecycles (Erhebung / Anpassung / Löschung ohne Dateninhalt)	

* Highlevel Sicht. Details je Fall sind in den weiteren Themen dieses Themengebiets behandelt
** Variablen S, P, L, R bedeuten, dass es sich um die jeweils betreffende Stelle / Prozess / Leistung / Rechtsgrundlage handelt und nicht aggregiert über bspw. alle Stellen. Stelle S wäre bspw. das Amt, welches auf die Daten zugegriffen oder diese genutzt hat.
*** Definition Typ siehe «Definition der nachvollziehbaren Personendaten»
**** Entspricht einer Automatisierung des Einsichtsrechts gemäss DSG

Abbildung 13: Übersicht der Themen des Themengebiets «Auskunft über Daten, Verwendung und Weitergabe», sowie deren Ausprägungen unterteilt in «in Scope» und «out-of Scope»

A.2.3. Welche Information zur Daten Verwendung werden dem Nutzenden geben

Die Aufteilung in «in scope» und «out of scope» wurde basierend auf den folgenden zwei Kriterien getroffen:

- Wird mit dieser Ausprägung der Bedarf der natürlichen Personen erfüllt?
- Ist diese Ausprägung aus offensichtlichen Gründen nicht oder nur schwer umsetzbar?

Für natürliche Personen von Interesse sind insbesondere:

- ob und welche Daten bei der Verwaltung über sie vorhanden sind
- ob und wieso (Zweck) diese Daten genutzt wurden
- ob und wie diese Daten weitergegeben wurden
- ob und wann diese Daten durch die Verwaltung verändert wurden

Bei der Berechtigung gibt es zwei verschiedene Aspekte:

- Rechtliche Erlaubnis, die Daten zu nutzen / weiterzugeben: ist für Nutzende zu generisch und erfüllt dadurch den Bedarf nicht (siehe auch nächste Folie)
- Erlaubnis des Nutzenden, diese Daten für andere als die gesetzlich zugelassenen Anwendungsfälle zu nutzen (siehe Folie «Anzustrebender Zusatznutzen für nat. Personen»)

Aggregierte und anonymisierte Daten können per Definition nicht mehr einer Person zugeordnet werden, weshalb die technische Machbarkeit nicht gegeben ist.

Bei dieser Gliederung handelt es sich um eine high-level Sicht. Die Details je Interessen Thema werden in den folgenden Abschnitten behandelt.

A.2.4. Details zur Nutzung

Um die Vision zu erreichen ist es entscheidend, dass die Nachvollziehbarkeitslösung Vertrauen schafft (und nicht umgekehrt Unsicherheit schürt): Die Nachvollziehbarkeitslösung soll Antworten liefern und nicht zusätzliche Fragen / Unklarheiten generieren. Nebst dem Erreichen des Hauptzwecks, der Stärkung des Vertrauens, werden damit auch zeitaufwändige Rückfragen im laufenden Betrieb reduziert.

Entsprechend sollen die zum Thema «Nutzung» gelieferten Informationen folgende vier Fragen beantworten:

- Wer hat auf die Daten zugegriffen → welche Stelle / Organisationseinheit hat auf die Daten zugegriffen?
- Zweck des Datenzugriffs → für welche/n (Verwaltungs-)Leistung/Prozess[84] wurde auf die Daten zugegriffen?
- Wann wurde auf die Daten zugegriffen → Historischer Verlauf, siehe separates Thema «historischer Verlauf (wann)»
- Basierend auf welchen Grundlagen wurde auf die Daten zugegriffen → basierend auf welcher Rechtsgrundlage wurde der Datenzugriff getätigt?

[84] eCH-0126 unterscheidet zwischen Prozessen und Leistungen. Ein Prozess (bspw. Einreichen Baugesuch) ist demnach in verschiedene Leistungen aufgeteilt. Für natürliche Personen dürften üblicherweise der Prozess interessanter sein als die Leistungen.

A.2.5. Details zur Datenweitergabe (verwaltungsintern, wie -extern)

Die «Weitergabe» und die «Entgegennahme» von Daten wird hier explizit unterschieden, da es mindestens für eine Übergangzeit Systeme geben wird, welche nicht Teil der Nachvollziehbarkeitslösung sein werden

Für die Granularität der Informationen bezüglich der Datennutzung durch die Verwaltung wurden folgende Stufen gewählt:

- Daten Weitergabe erlaubt → kein ausreichender Mehrwert gegenüber dem Status Quo und daher «out of Scope»
- Daten einer spezifischen Person weitergegeben → minimale Anforderung und daher «in Scope»
- Information über weitergegebene Daten-Kategorien → aus Sicht Kundschaft wünschenswert und daher «in Scope»
- Inhalt der weitergegebenen Daten → aus Sicht der Kundschaft wünschenswert, aufgrund von Komplexität und Speicherplatzbedarf vorderhand als «out of Scope» definiert
- Information bezüglich des Zwecks der Datenweitergabe (i.e. welche «Verwaltungsleistung») → notwendig, um die Datenweitergabe interpretieren zu können und daher «in Scope»
- Für natürliche Person ist der Prozess / die Leistung relevanter als die zugrunde liegende Rechtsgrundlage

A.2.6. Details zu gespeicherten Daten

Bei den Details zu den von der Verwaltungseinheit gespeicherten Personendaten stellt sich die Frage, wie viele Informationen rund um die Daten den Nutzenden geliefert werden sollen.

- Im optimalen Fall können dieselben Informationen wie bei einer Dateneinsicht gemäss Datenschutzgesetz geliefert werden. Das Einsichtsrecht könnte somit automatisiert werden.
- Bei der Anzeige insbesondere von Metadaten oder einer Teilsicht von Daten muss darauf geachtet werden, dass diese von den Nutzenden korrekt interpretiert werden können. Ansonsten besteht die Gefahr, dass anstatt Transparenz neue Fragen und Unsicherheiten generiert werden.

A.2.7. historischer Verlauf (wann)

Für Informationen zur Nutzung der Daten und der Datenweitergabe ist ein historischer Verlauf zwingend notwendig (die Aussage «gerade jetzt nutzt niemand Ihre Daten» bringt keinen Mehrwert).

Beim Inhalt der Daten gibt es mehrere Optionen:

- der aktuelle Datenbestand wird angezeigt
- der aktuelle Datenbestand inklusive Informationen zum Life-Cylcle wird angezeigt (bspw: zuletzt angepasst am, erstellt am, gelöscht am, ...)
- der aktuelle Datenstand sowie jeder Datenstand in der Vergangenheit werden angezeigt

Eine Auskunft über die komplette Historie des Dateninhalts (z.B. Angabe der Adresse von jedem Umzug im Verlauf des Lebens) wurde bewusst «out of Scope» gesetzt: Der Mehraufwand ist signifikant, ohne dass für den Nutzenden ein relevanter Mehrwert entsteht. Wo notwendig ist diese «Historisierung» von Daten in den Quellsystemen implementiert und steht im Bedarfsfall für verwaltungsinterne Nachforschungen zur Verfügung.

A.2.8. Definition der zu nachvollziehenden Personendaten

Teil dieses Themengebietes ist das Thema «Nachvollziehbare Personendaten». Die Abbildung 14 zeigt die Details dieses Themengebiets auf.

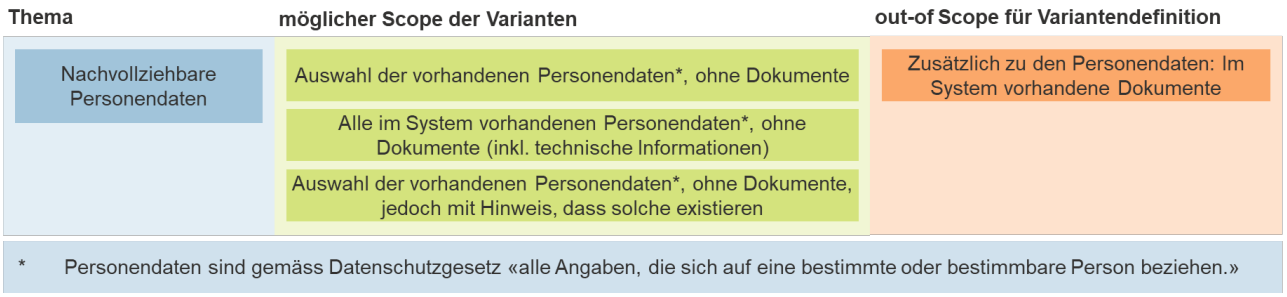

Abbildung 14: Übersicht der Themen des Themengebiets «Definition der zu nachvollziehenden Personendaten»

Folgende Punkte sollen bei der Ausformulierung der Lösungsansätze beachtet werden:

- Es sollen den Interessierten natürlichen Personen die Personendaten präsentiert werden, welche für diese den grössten Nutzen bezüglich der Transparenz bringen. Dies sind prinzipiell Daten, welche von den Nutzenden als «besonders sensitiv» eingestuft werden.
- Eine naheliegende Kategorisierung von Personendaten wird vom Datenschutzgesetz vorgegeben: «besonders schützenswerte» Personendaten und «alle anderen» Personendaten. Diese Kategorisierung ist für das Datenschutzgesetz ausreichend, für UZ13 könnte eine feinere Granularität sinnvoll sein, da beispielsweise «Steuerdaten» nicht als «besonders schützenswerte» Personendaten klassifiziert sind, von einer Mehrheit der natürlichen Personen jedoch als sensitiv eingestuft werden dürften.
- Der Kontext eines Datenzugriffs durch eine Verwaltungseinheit spielt eine wichtige Rolle: Greift das zuständige Amt für «kirchliche Angelegenheiten» auf die «Religionszugehörigkeit» zu (ein besonders schützenswertes Personendatum), wird dies im Allgemeinen wohl als eher unkritisch beurteilt. Greift der Nachrichtendienst des Bundes auf diese Information zu, so könnte dies von den Nutzenden eher als kritisch beurteilt werden.
- Für den Scope wurde die Entscheidung getroffen, dass auch die Option «volle Transparenz» (i.e. alle Personendaten werden angezeigt, sofern dies nicht gesetzlich eingeschränkt ist) im Sinne des Datenschutzgesetzes untersucht werden soll. Je nach anzubindenden (Fach)Systemen dürfte diese Option jedoch nur schwierig umsetzbar sein, da bestimmte systeminterne technische Informationen für die Nutzenden nicht ausreichend verständlich sein könnten.

Der Scope beschränkt sich bewusst auf strukturierte Datensammlungen wie Beispielsweise Datenbanken. Dokumente, welche Personendaten enthalten, wurden bewusst vom Scope ausgeschlossen. Dies, da eine Identifikation der relevanten Dokumente mit einer viel höheren Komplexität und entsprechendem Aufwand verbunden ist. Zudem müsste sichergestellt werden, dass in den Dokumenten keine Personendaten Dritter oder sonstige schützenswerte Informationen enthalten sind.

A.2.9. Stufe bis zur welcher eine Nachvollziehbarkeit erfolgt

Teil dieses Themengebietes ist das Thema «Nachvollziehbarkeit bis auf Stufe». Die Abbildung 15 zeigt die Details dieses Themengebiets auf.

Thema	möglicher Scope der Varianten	out-of Scope für Variantendefinition
Nachvollziehen bis auf Stufe	Verwaltungseinheit* Mitarbeiter, welcher auf Daten zugreift, für natürliche Person nicht einsehbar	Mitarbeiter, welcher auf Daten zugreift, für natürliche Person einsehbar

* Mit Verwaltungseinheit ist die organisatorische Einheit gemeint, welcher ein Mitarbeiter zugehört, der eine Aktion auf einem System vorgenommen hat (bspw. Direktion, Amt, Abteilung, Sektion).

Abbildung 15: Übersicht der Themen des Themengebiets «Stufe bis zur welcher eine Nachvollziehbarkeit erfolgt»

Es werden zwei Stufen unterschieden, bis auf welche eine Handlung mit Daten nachvollzogen werden kann:

- Die unterste Organisationsebene in welcher der Mitarbeitende (oder das System) angesiedelt ist, welcher die Handlung mit den Personendaten der betroffenen Person durchgeführt hat. Wobei bei kleinen Organisationseinheiten eine übergeordnete Organisationseinheit gewählt werden müsste, falls die die Anonymität der Mitarbeitenden sichergestellt werden soll[85].
- Der Mitarbeitende (oder das System), welcher eine Aktion mit Personendaten der betroffenen Person durchgeführt hat.

Hierbei gilt es eine Güterabwägung zwischen dem Interesse des Nutzenden an Transparenz und dem Interesse des Verwaltungs-Mitarbeitenden der nach Schutz seiner Person durchzuführen. Es ist daher sinnvoll, einen möglichen Mittelweg zu definieren: Der Nutzende der Nachvollziehbarkeitslösung bekommt keine Einsicht, welcher Verwaltungs-Mitarbeitende die Daten bearbeitet hat. Die Information zum Mitarbeitenden wird jedoch systemintern vorgehalten, um im Falle eines potentiellen Missbrauchs die notwendigen Informationen zur Verfügung zu haben.

A.2.10. Anzustrebender Zusatznutzen für natürliche Personen

Teil dieses Themengebietes ist das Thema «Zusatznutzen für natürliche Personen». Die Abbildung 16 zeigt die Details dieses Themengebiets auf.

Thema	möglicher Scope der Varianten	out-of Scope für Variantendefinition
Zusatznutzen für nat. Personen	Einsicht Kontaktadresse zuständige Verwaltungseinheit (Postadresse / Telefon / Email)	Erfassung / Korrektur Daten pro Verwaltungseinheit zentrale Erfassung / Korrektur Daten (Once Only Teilaspekt) Nutzungsfreigabe für Verwaltungseinheiten, welche keinen rechtlichen Anspruch auf Daten haben Nutzungsfreigabe für Dritte, welche keinen rechtlichen Anspruch auf Daten haben Möglichkeit zur Beschwerde bezüglich Datennutzung

[85] Die rechtliche Abwägung zwischen dem Schutz des Mitarbeitenden und dem Transparenzgebot der öffentlichen Verwaltung muss im Einzelfall geprüft werden.

Abbildung 16: Übersicht der Themen des Themengebiets «Anzustrebender Zusatznutzen für natürliche Personen»

Der mit dieser Lösung umgesetzte Hauptnutzen für natürlichen Personen ist die Nachvollziehbarkeit der Verwendung persönlicher Daten, womit das Vertrauen in die digitale Verwaltung gestärkt werden soll. Nebst diesem Hauptnutzen könnte potentiell aktiv angestrebt werden, auch weiterer Nutzen für natürlichen Personen umzusetzen.

Nach dem Credo, «weniger ist mehr», wurde entschieden, den Fokus auf den Hauptnutzen zu setzen.

Einzig soll dem Nutzenden die Kontaktadresse der für ein System zuständige Verwaltungseinheit (Postadresse / Telefon / E-Mail) mit der Datenauskunft als Zusatznutzen mitgeliefert werden. Damit können die Nutzenden bei Fragen oder Unstimmigkeiten direkt die zuständige Verwaltungseinheit kontaktieren.

Weitere identifizierte Zusatznutzen sollen nicht durch UZ13, sondern durch andere Projekte und Initiativen umgesetzt werden. Falls der Lösungsvorschlag Zusatznutzen sowieso liefert, werden diese selbstverständlich berücksichtigt

A.2.11. Anzustrebender Zusatznutzen für öffentliche Verwaltung

Teil dieses Themengebietes ist das Thema «Zusatznutzen für die öffentliche Verwaltung». Die Abbildung 17 zeigt die Details dieses Themengebiets auf.

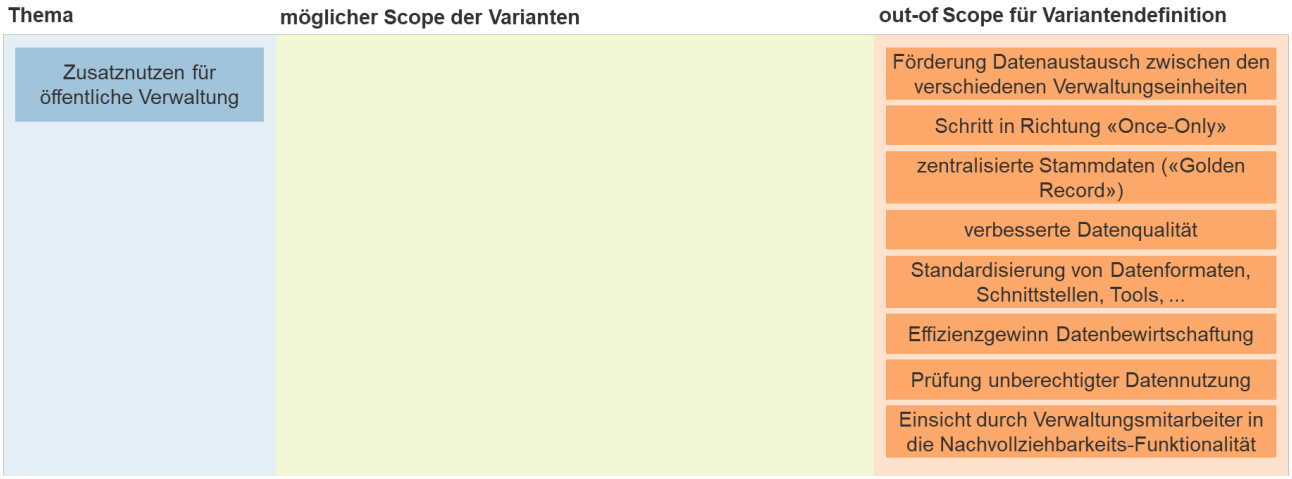

Abbildung 17: Übersicht der Themen des Themengebiets «Anzustrebender Zusatznutzen für die öffentliche Verwaltung»

Ein aktiv anzustrebender, potentieller Zusatznutzen für die öffentliche Verwaltung, welcher im Rahmen einer Nachvollziehbarkeitslösung mit Zusatzaufwand umgesetzt werden könnte, wurde bewusst als «out of Scope» deklariert. UZ13 soll sich auf die Kernziele fokussieren. Weitere identifizierte Zusatznutzen sollen nicht durch UZ13, sondern durch andere Projekte und Initiativen umgesetzt werden. Falls der Lösungsvorschlag per se einen Zusatznutzen liefert, wird dieser selbstverständlich berücksichtigt.

A.2.12. In die Nachvollziehbarkeitslösung einzubindende Systeme

Das Themengebiet «In die Nachvollziehbarkeitslösung einzubindende Systeme» ist in drei Themen gegliedert. Abbildung 18 zeigt die Details dieses Themengebiets auf.

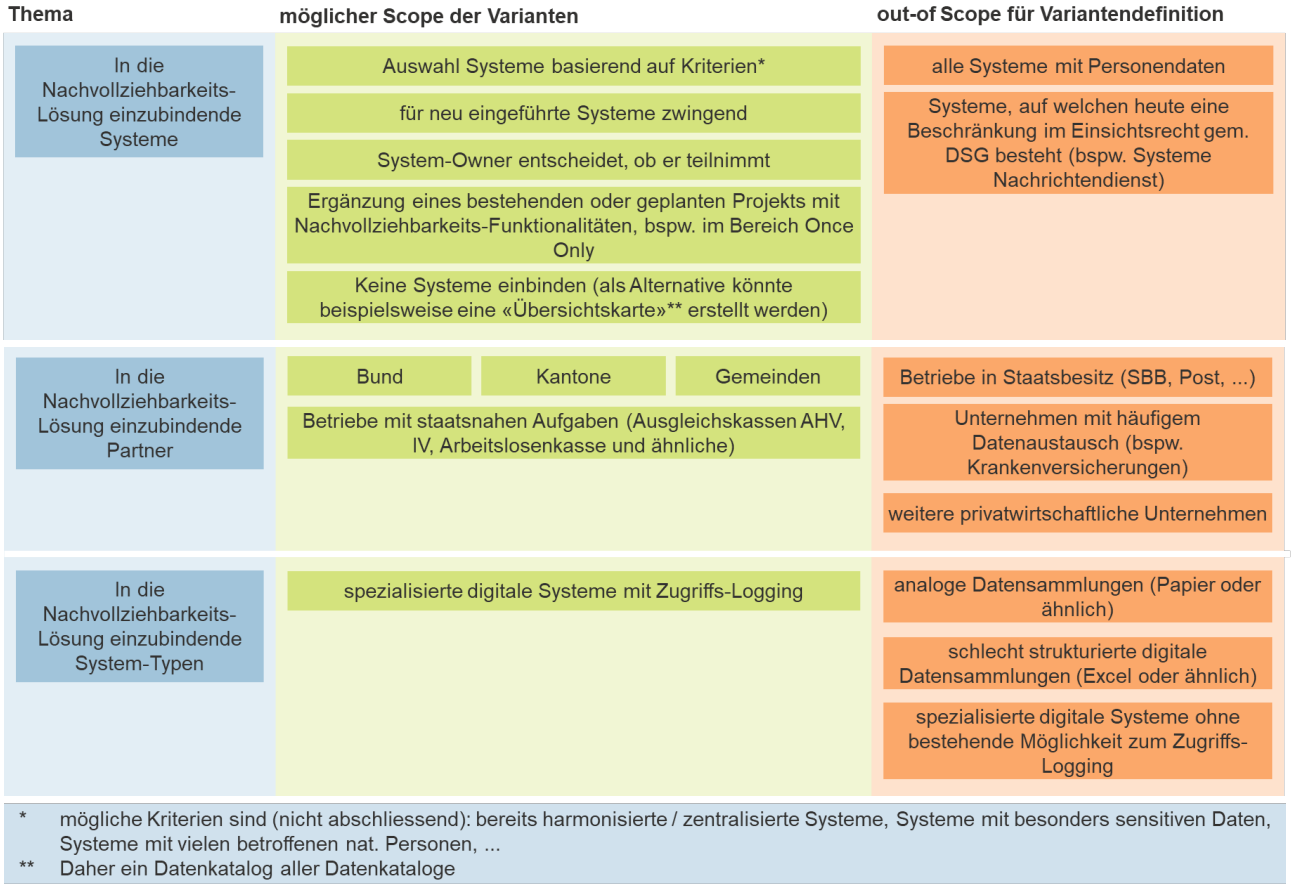

Abbildung 18: Übersicht der Themen des Themengebiets «In die Nachvollziehbarkeitslösung einzubindende Systeme»

A.2.13. In die Nachvollziehbarkeitslösung einzubindende Systeme

Eine grobe Analyse zeigt auf, dass schweizweit mehr als 10'000 Systeme von Verwaltungseinheiten auf den verschiedenen Staatsebenen existieren, welche Personendaten enthalten. In einer kurz- und mittelfristigen Perspektive ist es unrealistisch, sämtliche Systeme an die Nachvollziehbarkeitslösung anzubinden.

Aus Sicht des Nutzenden ist es wünschenswert, wenn möglichst viele der für die jeweilige natürliche Person relevanten Systeme in die Nachvollziehbarkeitslösung eingebunden werden.

Es stellt sich die Frage, ob die Anbindung von «einer Hand voll» Systemen an die Nachvollziehbarkeitslösung für die Nutzenden einen signifikanten Mehrwert im Bereich der Transparenz schafft.

Die verschiedenen präsentierten Kategorien schliessen sich nicht alle gegenseitig aus und können teilweise kombiniert werden.

Es gibt heute bereits Systeme (beispielsweise des Nachrichtendienstes und der Strafverfolgung), in welche kein Einsichtsrecht gemäss Datenschutzgesetz besteht. Im Rahmen des UZ13 werden keine rechtlichen Änderungen angestrebt, um dies zu ändern.

Eine Priorisierung von Systemen bei der Anbindung an die Nachvollziehbarkeitslösung kann entlang von verschiedenen Achsen vorgenommen werden (folgende Liste ist nicht abschliessend):

- geringer Aufwand zur Anbindung
- System mit grosser Anzahl Datensätzen über verschiedene natürliche Personen

- System mit besonders sensitiven Personendaten

Anstatt eine losgelöste Nachvollziehbarkeitslösung neu aufzubauen, könnte die notwendige Funktionalität als Teil eines anderen Projekts (bspw. im Bereich «Once Only») umgesetzt werden. Dieser Ansatz wurde beispielsweise in Estland mit «My Tracker» als Teil der nationalen Datenaustausch-Architektur «X-Road» und in Dänemark mit «Mit Overblik» als Teil des Bürgerportals gewählt.

«Keine Systeme einbinden»: Als Alternative könnte beispielsweise ein verwaltungsübergreifender Datenkatalog erstellt werden, in welchem sämtliche Systeme aufgeführt sind, in welchen Personendaten gespeichert werden (inkl. den bereits heute beispielsweise auf Bundesstufe verfügbaren Zusatzinformationen). Diese Lösung deckt die Anforderungen der Nutzenden nicht ausreichend ab.

A.2.14. In die Nachvollziehbarkeitslösung einzubindende Partner

Gemäss der verabschiedeten Vision liegt der Fokus auf der Stärkung des Vertrauens in die digitale Verwaltung. Die Auswahl der einzubindenden Partner folgt der Vision. Es handelt sich um Gemeinden, Kantone, Bund und Organisationen mit staatsnahen Aufgaben[86]. Folgende mögliche Partner wurden bewusst als «out of Scope» definiert:

- Betriebe in Staatsbesitz (SBB, Post, ...)
- Unternehmen mit häufigem Datenaustausch mit der Verwaltung. Dazu zählen beispielswiese Krankenversicherungen, wobei der Datenaustausch zwischen diesen und der Verwaltung gesetzlich geregelt ist
- weitere privatwirtschaftliche Unternehmen

Werden Daten von einem an die Nachvollziehbarkeitslösung angeschlossenen System an ein externes System geteilt (beispielsweise im Bereich der Krankenkassen), so besteht je nach gewählter Variante die Möglichkeit, dies entsprechend zu Loggen und gegenüber dem Nutzenden sichtbar zu machen.

Organisationen mit staatsnahen Aufgaben (Ausgleichskassen AHV, IV, Arbeitslosenkasse und ähnliche) sind explizit «in Scope», da diese teilweise sensitive Personendaten halten und damit potenziell ein grosser Bedarf der natürlichen Personen an Nachvollziehbarkeit besteht.

A.2.15. In die Nachvollziehbarkeitslösung einzubindende System-Typen

Bei den in der Nachvollziehbarkeitslösung einzubindenden System-Typen liegt der Fokus auf digitale Systeme mit gut strukturierten Datensätzen, die mit einem bestehenden Logging der Zugriffe ausgestattet sind.

Es ist nicht die Aufgabe von UZ13, bestehende Systeme zu modernisieren. Diese Systeme sollen separat durch die zuständige Verwaltungseinheit modernisiert werden:

- Bei analogen oder schlecht strukturierten digitalen Datensammlungen (bspw. Excel) ist der Aufwand zur Einbindung in die Nachvollziehbarkeitslösung gross und als Teil von UZ13 nicht zielführend.
- Selbiges gilt für Systeme, welche Daten strukturiert halten, jedoch keine Möglichkeit bieten, die Aktionen auf dem System zu loggen. Für Nutzende wäre nur schwer erkennbar, wieso gewisse Systeme die Verwendung anzeigen, andere jedoch nicht. Im Sinne der Transpa-

[86] Bspw. die AHV Ausgleichskassen.

renz sollen solche Systeme explizit nicht an die Nachvollziehbarkeitslösung angeschlossen werden.

A.3. Unterstützungsmassnahmen zum Auskunftsrecht von Bund und Kantonen

Tabelle 6: Übersicht Unterstützungsmassnahmen[87] zum Auskunftsrecht seitens Bund und Kanton[88]

Kanton	Beschreibung Rechte und Prozesse	Musterbriefe vorhanden	Zentrales öffentlich zugängliches Register der Datensammlungen	Zuganginformation
AG	x	-	-	https://www.ag.ch/de/dvi/ueber_uns_dvi/organisation_dvi/generalsekretariat/beauftragte_fuer_oeffentlichkeit_und_datenschutz/informationen_fuer_private/informationen_fuer_private_1.jsp
AR	-	-	x	https://www.ar.ch/verwaltung/datenschutz-kontrollorgan/register-der-datensammlungen/
AI	-	-	x	https://www.ai.ch/verwaltung/justiz-polizei-und-militaerdepartement/datenschutzbeauftragter
BL	-	-	-	
BS	x	-	-	https://www.dsb.bs.ch/datenschutz/welche-rechte-haben-sie.html
BE	x	-	x	https://www.jgk.be.ch/jgk/de/index/aufsicht/datenschutz/ihre_datenschutzrechte.html https://www.jgk.be.ch/jgk/de/index/aufsicht/datenschutz/register_der_datensammlungen.html
FR	x	-	x	https://www.fr.ch/de/institutionen-und-politische-rechte/transparenz-und-datenschutz/datenschutz https://www.fr.ch/institutions-et-droits-politiques/transparence-et-protection-des-donnees/registre-des-fichiers-refi
GE	x	x	x	https://www.ge.ch/ppdt/espace-citoyen/espace-citoyen.asp https://www.ge.ch/ppdt/espace-citoyen/catalogue.asp
GL	-	-	-	
GR	x	x	-	https://www.gr.ch/DE/institutionen/verwaltung/staka/FachstelleOeffentlichkeitsprinzip/Seiten/Fachstelle.aspx
JU	x	x	-	https://www.ppdt-june.ch/fr/Documentation/Modeles-Documents/PdD-Particuliers-AccesPerso-Acces-donnees/Demande-d-acces-a-ses-donnees-personnelles.html
LU	-	-	x	https://datenschutz.lu.ch/registerdatensammlung/Register_Datensammlungen
NE	x	x		https://www.ppdt-june.ch/fr/Documentation/Modeles-Documents/PdD-Particuliers-AccesPerso-Acces-donnees/Demande-d-acces-a-ses-donnees-personnelles.html
NW	x	x	x	https://www.kdsb.ch/xml_1/internet/de/application/d351/d352/f353.cfm https://www.kdsb.ch/xml_1/internet/de/application/d138/f141.cfm
OW	x	x	x	https://www.kdsb.ch/xml_1/internet/de/application/d351/d352/f353.cfm https://www.kdsb.ch/xml_1/internet/de/application/d138/f140.cfm
SH	-	-	-	
SZ	x	x	x	https://www.kdsb.ch/xml_1/internet/de/application/d351/d352/f353.cfm https://www.kdsb.ch/xml_1/internet/de/application/d138/f139.cfm
SO	x	x	-	https://so.ch/staatskanzlei/datenschutz-oeffentlichkeitsprinzip/oeffentlichkeitsprinzip/allgemeines/
SG	x	x	x	https://www.sg.ch/sicherheit/datenschutz/meine-rechte/kantonaler-datenschutz.html https://www.sg.ch/sicherheit/datenschutz/register-der-datensammlungen.html
TI	x	-	-	https://www4.ti.ch/can/sgcds/trasparenza/trasparenza/
TG	-	-	x	https://www.datenschutz-tg.ch/re/
UR	x	-	x	https://www.ur.ch/dienstleistungen/6140

[87] Stand der Recherche: November 2020. Die Autoren haben auf den jeweiligen Internetauftritten der Kantone die Information gesucht. Es kann nicht ausgeschlossen werden, dass gewisse Informationen durch die Autoren der Studie nicht gefunden wurden – in diesem Fall kann jedoch auch davon ausgegangen werden, dass eine Mehrheit der natürlichen Personen diese Informationen nicht gefunden hätte.

[88] Wobei «x» Ja bedeutet und «-» Nein

				https://www.ur.ch/publikationen/7680
VD	x	x	x	https://www.vd.ch/themes/etat-droit-finances/protection-des-donnees-et-droit-a-linformation/droit-a-linformation/ https://www.vd.ch/themes/etat-droit-finances/protection-des-donnees-et-droit-a-linformation/protection-des-donnees/registre-des-fichiers/
VS	x	-	x	https://www.vs.ch/de/web/che/lipda https://www.vs.ch/de/web/che/registre-des-fichiers
ZG	x	x	x	https://www.zg.ch/behoerden/datenschutzstelle/ihre-rechte/auskunftsrecht
ZH	x	x	-	https://www.zh.ch/de/politik-staat/datenschutz/meine-rechte.html
Bund	x	x	x	https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/ueberblick/das-auskunftsrecht.html https://www.datareg.admin.ch/

A.4. Übersicht über Kantonale E-Government Plattformen

Tabelle 7: Übersicht[89] kantonaler E-Government Plattformen mit Fokus natürliche Personen

Kanton	Plattform	Beschreibung / Funktionalität (potentiell für UZ 13 relevante Auswahl)
AG	Einzelanwendungen	• eUmzug • Baugesuche (Pilot)
AR	Einzelanwendungen	• eUmzug • eGrundbuch
AI	keine	
BL	keine (Online Schalter mit Online Formulare)	
BS	eKonto[90]	• eUmzug • Ordnungsbussen • Bezug Dokumente (Trauungsurkunde, …) • Arbeits- / Grenzgängerbewilligung
BE	BE-Login[91]	• Steuererklärung • Betreuungsgutscheine • Baubewilligung • Zugang Grundbuch • Anmeldung Handelsregister
FR	Virtueller Schalter[92] basierend auf iGovPortal	• Bezug Dokumente (Betreibungsregister, Handelsregister, Zivilstandsdokumente) • Fischereipatente • Weitere in Planung (eUmzug, Schulzeugnisse, Handelsreistereintrag, Grundbuchauszüge, Betreibungsbegehren)
GE	e-démarches[93]	
GL	keine (Online Schalter mit Online Formulare)	
GR	keine (Online Schalter bietet online Bezahlung von Ordnungsbussen an)	
JU	Guichet virtuel[94] basierend auf iGovPortal	• Steuererklärung • Klagen und Insolvenzen • Services des Strassenverkehramtes • Jagd- und Fischereipatente
LU	keine (Online Schalter mit Online Formulare)	
NE	Guichet Unique[95]	• Gebäudeversicherungsverträge • Services rund um Tiere, Kultur, Schulen, Grundsteuern • Klagen und Insolvenzen • Services des Strassenverkehramtes • Jagd- und Fischereipatente
NW	Einzel Anwendungen, zusätzlich Online Schalter mit Online Formulare	• Steuererklärung
OW	keine (Online Schalter mit Online Formulare)	

[89] Stand der Recherche: November 2020. Die Autoren haben auf den jeweiligen Internetauftritten der Kantone die Information gesucht. Es kann nicht ausgeschlossen werden, dass gewisse Informationen durch die Autoren der Studie nicht gefunden wurden – in diesem Fall kann jedoch auch davon ausgegangen werden, dass eine Mehrheit der natürlichen Personen diese Informationen nicht gefunden hätte.

[90] Siehe: https://konto.egov.bs.ch/auth/login

[91] Siehe: https://www.belogin.directories.be.ch/cms/de/welcome.html

[92] Siehe: https://www.fr.ch/de/alltag/vorgehen-und-dokumente/online-dienste

[93] Siehe: https://www.ge.ch/catalogue-e-demarches

[94] Siehe: https://guichet.jura.ch/

[95] Siehe: https://www.guichetunique.ch/

SH	eGov Box[96] sh.sh[97]	• Services rund um Bescheinigungen, Umzug, Steuern (ohne Online-Steuererklärung), sowie diverse weitere
SZ	keine (Online Schalter mit Online Formulare)	
SO	Online Schalter[98] basierend auf iGovPortal	• Services rund um den Bezug von Auszügen
SG	eGov Box[99] basierend auf iGovPortal	• Services rund um Bescheinigungen, Umzug, Steuern (ohne Online-Steuererklärung)
TI	keine (Online Schalter mit Online Formulare)	
TG	keine	
UR	Online Schalter[100]	
VD	Cyberadministration[101]	
VS	Keine (Online Schalter mit Online Formulare)	
ZG	Keine (Online Schalter mit Online Formulare)	
ZH	ZHservices[102]	• Steuererklärung • Gesuche Militär und Zivilschutz

[96] Siehe: https://eservices.sh.ch/

[97] Siehe: https://sh.ch/CMS/Webseite/Kanton-Schaffhausen/Beh-rde/Services/Dienstleistungs-Portal-2207-DE.html

[98] Siehe: https://my.so.ch/

[99] Siehe: https://eservices.vrsg.ch/public/web/sg/portal/

[100] Siehe: https://www.ur.ch/online-schalter

[101] Siehe: https://www.vd.ch/cyberadministration-acces-aux-prestations-en-ligne/

[102] Siehe: https://www.services.zh.ch/

A.5. Prozesse in der Verwaltung

Der Standard eCH-0203[103] gibt eine Übersicht über die verschiedenen eCH-Standards im Bereich der «vernetzten Verwaltung der Schweiz» und fasst die Ergebnisdokumente der eCH-Fachgruppe Geschäftsprozesse zusammen. Geschäftsprozesse können alle drei Staatsebenen involvieren. Als Beispiel dafür ist wiederum die jährliche Steuererhebung genannt: Die natürliche Person reicht typischerweise beim Kanton oder der Gemeinde (je nach Wohnort) ihre Steuererklärung ein und bezahlt die Steuern für alle drei Staatsebenen. Entsprechend erstreckt sich der für die Ausführung der betroffenen Prozesse benötigte Datenaustausch über alle drei Staatsebenen.

Weiter können innerhalb einer Staatsebene verschiedene Akteure in einen Prozess involviert sein. Ein solches Beispiel wird im Standard eCH-0126 dargestellt. Der Standard beschreibt zwei mögliche generische Formen des Baubewilligungsprozesses. In beiden Fällen besteht mindestens eine Interaktion mit der natürlichen Person[104] und es sind mehrere Verwaltungseinheiten involviert. Abbildung 19 zeigt eine Prozessvariante, in welcher die natürliche Person selbständig mit den verschiedenen betroffenen Stellen der öffentlichen Verwaltung einzeln in Kontakt tritt. Der Aufwand für die natürliche Person ist in dieser Prozessvariante relativ hoch. Im Gegenzug hat die natürliche Person eine gute Einsicht, was mit den bereitgestellten Personendaten gemacht wird. Abbildung 20 zeigt eine Prozessvariante, in welcher der Aufwand für die natürliche Person minimiert wird, indem die verschiedenen Verwaltungseinheiten als einheitlicher Dienstleister gegenüber dieser auftreten. Die Prozess-Zwischenschritte laufen grösstenteils automatisch und ohne Kontakt zur natürlichen Person ab. Als Resultat davon hat die natürliche Person einen weniger guten Einblick über die verwaltungsinternen Prozessschritte und damit über die Verwendung der Personendaten durch die öffentliche Verwaltung. In der Tendenz werden Verwaltungs-Prozesse je länger je mehr entlang der zweiten Variante aufgebaut – die öffentliche Verwaltung wird zum Dienstleister, die natürliche Person zur Kundin oder zum Kunden.

Aus den aufgeführten Prozessbeispielen ergeben sich folgende Erkenntnisse:

- Für die erfolgreiche Abwicklung eines Prozesses werden teilweise innerhalb einer Staatsebene mehrere Verwaltungseinheiten, resp. sogar Verwaltungseinheiten mehrerer Staatsebenen benötigt und involviert.
- Sobald die verschiedenen Prozessschritte durch die Verwaltung selbst angestossen und abgewickelt werden, ist es für die natürliche Person schwer respektive sogar unmöglich nachzuvollziehen, welche Verwaltungseinheit wann welche Daten wieso erhält, nutzt, verändert und wiederum weitergibt, sowie welche Stellen auf diese Daten zugreifen.

In Abbildung 20 wird auch der Zusammenhang zwischen «Leistung» und «übergeordnetem Prozess» gemäss der Definition von eCH illustriert: Ein Prozess besteht aus einer oder mehrere Leistungen.

[103] Siehe: https://www.ech.ch/de/dokument/537d1f01-addf-4828-9e49-df099b576b7e

[104] eCH-0126 spricht nicht von natürlichen Personen sondern verwendet den Begriff «Kunden», in welchem auch juristische Personen eingeschlossen sind.

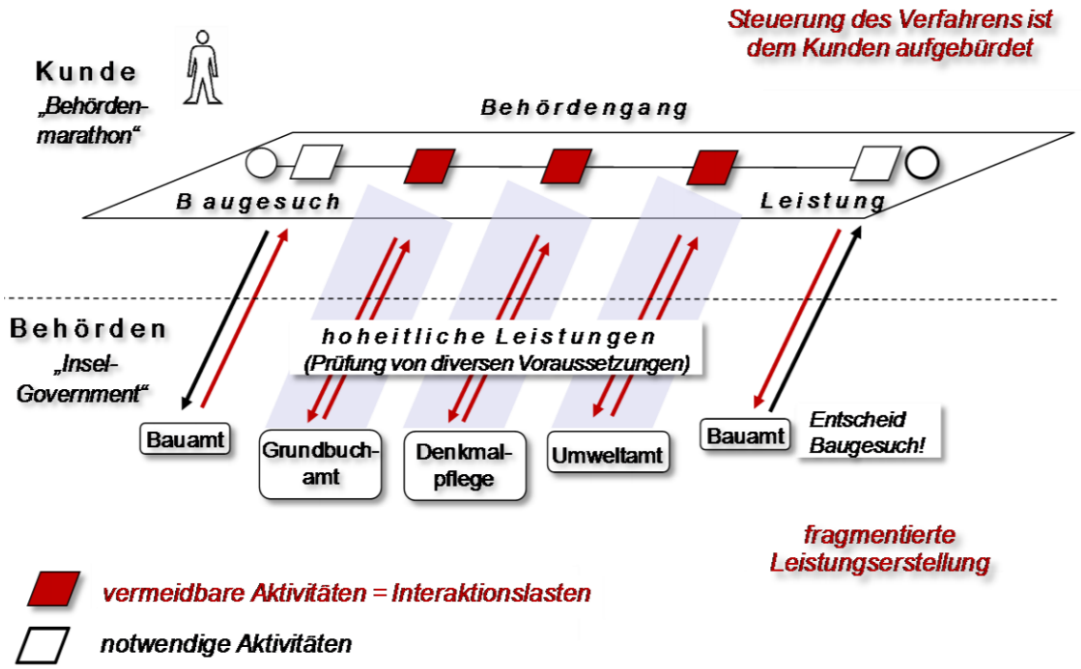

Abbildung 19: Prozess Baugesuch bei siloartiger Organisation der Gemeinde[105]

Der Standard eCH-0176[106] geht noch einen Schritt weiter, indem Prozesse der öffentlichen Verwaltung entlang von vier Referenzmodellen optimiert werden sollen:

- **Föderales Kooperationsmodell:** Die zuständigen Stellen bleiben weiterhin zuständig, einigen sich aber gemeinsam, wer welche Leistungen zu einem Prozess beisteuert.
- **Konzept der Leistungsarchitekturen**: Die Leistungsarchitektur erlaubt eine Verwaltungsübergreifende gemeinsame Beschreibung von notwendigen Leistungsbausteinen für die Leistungserbringung.
- **Konzept der Prozessmodularisierung**: Gewisse Prozessmodule werden von der zuständigen Stelle an eine Dritt-Stelle ausgelagert, um die Effizienz zu steigern.
- **Konzept der Prozessoperationalisierung:** Detaillierte Erfassung sämtlicher Prozessschritte mit dem Ziel, ähnliche Prozessschritte zusammenzulegen und dadurch Skaleneffekte zu erreichen.

[105] eCH-0126 siehe: https://www.ech.ch/de/dokument/fa1c7c13-60bc-4ca5-8b81-ee66f689c0d1

[106] eCH-0176 siehe: https://www.ech.ch/de/dokument/a1271500-ff87-4a73-9a65-778253009947

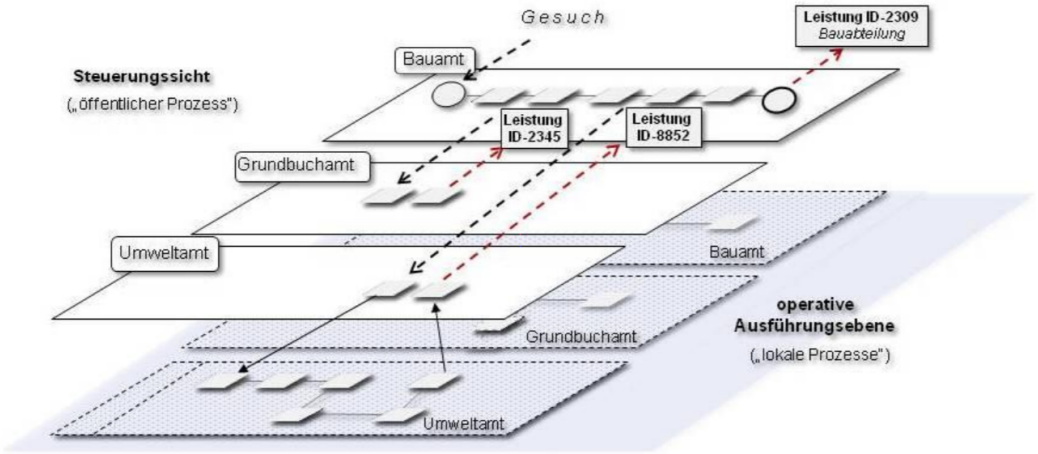

Abbildung 20: Prozess Baugesuch mit "übergreifender Leistungserstellung" nach eCH-0126

A.6. Standardisierung nach eCH

Abbildung 21 gibt einen Überblick über Themen, in welchen eCH Standardisierungen vorgenommen hat. Das Vorhandensein von Standards bedeutet nicht, dass die Themen vollständig standardisiert sind, sondern lediglich, dass Aspekte davon standardisiert wurden Es gibt nicht für alle Themenbereiche mit Relevanz zu Personendaten explizite Standards (bspw. die Bereiche «Arbeit» und «Bildung»[107] fehlen). Teilweise werden die Bereiche durch allgemein gültige Standards abgedeckt. Für Bereiche ohne Standardisierung durch eCH oder andere Gremien bedeutet dies, dass die in den Systemen der verschiedenen Verwaltungen gespeicherten Personendaten im Allgemeinen weder standardisiert noch harmonisiert sind[108]. Dieser potentiell grosse Umfang an nicht standardisierten Daten wirkt je nach Variante erschwerend auf eine mögliche Umsetzung einer Nachvollziehbarkeitslösung. Tabelle 8 zeigt eine Auswahl relevanter eCH Datenstandards mit Bezug zu UZ13.

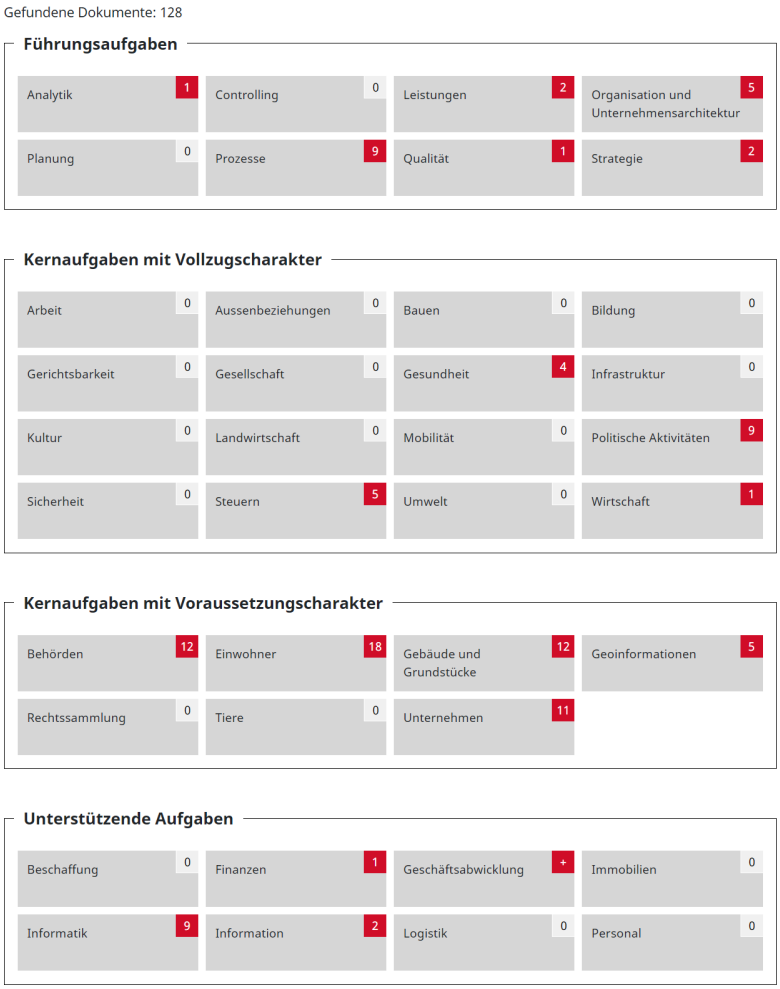

Abbildung 21: Übersicht über eCH Standards (Stand Ende 2020)

[107] Die Fachgruppe «Bildung» wurde relativ neu geschaffen: https://www.ech.ch/de/node/54161

[108] Für die Begriffe «Standardisierung» und «Harmonisierung» wird die Bedeutung gemäss NaDB / IOP des BFS verwendet:
Standardisierung: Definition eines allgemein gültigen Standards
Harmonisierung: Zusammenführen der bisher vorhandenen Daten in eine Form, dass diese dem Standard folgen und eine einheitliche Bedeutung haben.

Tabelle 8: eCH Datenstandards mit einem direkten Zusammenhang zu Personendaten

Nummer	Titel
eCH-0006	Datenstandard Ausländerkategorien
eCH-0010	Datenstandard Postadresse
eCH-0011	Datenstandard Personendaten
eCH-0021	Datenstandard Personenzusatzdaten
eCH-0044	Datenstandard Austausch von Personenidentifikationen
eCH-0046	Datenstandard Kontakt
eCH-0135	Datenstandard Heimatort
eCH-0136	Datenstandard Zuständigkeiten im Zivilstandwesen
eCH-0156	Datenstandard ISA-Datenimport aus den Einwohnerregistern
eCH-0185	Datenstandard Zusatzdaten Wegzug / Zuzug
eCH-0234	SHIP Datenstandard Leistungsfälle Administration Gesundheitswesen

A.7. Plattformen zum Datenaustausch

A.7.1. sedex (CH)

sedex steht für *secure data exchange* und ist eine Dienstleistung des Bundesamts für Statistik BFS. Die Plattform ist für den sicheren asynchronen Datenaustausch zwischen Organisationseinheiten konzipiert. Bei Bedarf können Daten mittels sedex auch synchron ausgetauscht werden. Die Plattform ist hochverfügbar.

sedex wurde im Rahmen der Modernisierung der Volkszählung aufgebaut, um die Statistiklieferungen der kommunalen Einwohnerdienste und der Personenregister des Bundes an das BFS sicherzustellen. Da sensitive Daten ausgetauscht werden, musste die Plattform von Beginn an hohen Anforderungen an die Sicherheit sowie Nachvollziehbarkeit genügen. Dazu setzt sedex moderne Verschlüsselungsverfahren sowie Sicherheitszertifikate der Swiss Government PKI ein.

Seit Inbetriebnahme Mitte 2008 hat sich sedex auch Teilnehmern ausserhalb der Registerharmonisierung und der Statistik geöffnet. Heute wird sedex von über 7'700 Organisationseinheiten[109] eingesetzt. Im Jahr 2018 wurden ca. 17.6 Millionen Meldungen, im Jahre 2019 22.5 Millionen via sedex übermittelt. sedex ist damit die meistgenutzte Plattform in der Schweiz mit dem erwähnten Zweck.

Die Meldungen werden via der sedex-Plattform beim BFS ausgetauscht und durch den sendenden Client verschlüsselt, wobei dies so konzipiert ist, dass nur der Empfänger in der Lage ist, die Daten zu entschlüsseln. Heute gibt es ca. 650 verschiedene Meldungstypen, wobei jeder Meldungstyp in der Regel einem Geschäftsfall entspricht, der zwischen den sedex-Teilnehmern abgewickelt wird.

Basierend auf sedex werden auch Abfrage-Services wie beispielsweise die «Schnittstelle UPI-Services» für Abfragen im UPI-Register (Unique Person Identification) angeboten[110] [111].

A.7.2. ELM (CH) / Verein Swissdec

ELM steht für einheitliches und zertifiziertes Lohnmeldeverfahren und bietet eine Plattform für den verschlüsselten elektronischen Austausch von Lohndaten zwischen Unternehmen (direkt aus dem ERP-System) und Lohndatenempfänger wie der AHV, BVG-Versicherer, Steuerverwaltungen (Lohnausweis, Quellensteuer), BFS (schweizerische Lohnstrukturerhebung) sowie den Unfall- und Krankentaggeld-Versicherern.[112]

A.7.3. Plattformen für die sichere Zustellung im Rahmen von rechtlichen Verfahren (CH)

Für die elektronische Übermittlung im Rahmen von Zivil- und Strafprozessen sowie von Schuldbetreibungs- und Konkursverfahren sieht die Verordnung über die elektronische Übermittlung (VeÜ-ZSSV, SR 272.1) einen Versand über eine Zustellplattform vor, die eine vertrauliche, integre und nachvollziehbare Zustellung sicherstellt. Die Nachrichten werden in unstrukturierter Form übermittelt [113].

Vom Bund anerkannte Plattformen sind:

---

[109] Was Verbände, Vereinigungen, Kantone sowie Gemeinden oder Städte sein können

[110] Siehe: https://www.zas.admin.ch/zas/de/home/partenaires-et-institutions-/unique-person-identification--upi-/upiservices.html

[111] Der Text in diesem Abschnitt wurde in gekürzter und redigierter Form von der offiziellen sedex Homepage (http://www.sedex.ch/) übernommen, respektive mit aktuelleren Daten ergänzt.

[112] Details siehe: https://www.swissdec.ch/fileadmin/user_upload/_Promotionsmaterial/03904_d.pdf

[113] Der Text in diesem Abschnitt wurde in gekürzter und redigierter Form von der offiziellen Homepage zur elektronische Übermittlung (https://www.bj.admin.ch/bj/de/home/staat/rechtsinformatik/e-uebermittlung.html) übernommen.

- PrivaSphere Secure Messaging der Firma PrivaSphere AG
- IncaMail der Schweizerischen Post

A.7.4. HIN (Health Info Net)

Health Info Net (HIN) ist ein privates Unternehmen, welches sich auf den Datenaustausch im Medizinbereich spezialisiert hat[114]. Das Unternehmen bietet auch zertifizierte Identitäten (eID) als Kern seiner Dienstleistungen an[115].

A.7.5. X-Road (EU)

Die erste Version von X-Road wurde im Jahr 2001 in Estland entwickelt[116]. Sämtliche für X-Road notwendige Software ist komplett Open-Source[117]. Eine Datenanfrage von einem System wird per Security Server verschlüsselt an den Security Server des Systems weitergeleitet, welches den entsprechenden Service / die entsprechenden Daten anbietet. Zentrale Services stellen sicher, dass die Security Server vertrauenswürdig sind und dass die für einen Zugriff notwendigen Rechte vorhanden sind. X-Road wird heute in diversen Ländern eingesetzt[118] und kann auch zum Austausch von Daten zwischen verschiedenen Ländern verwendet werden[119].

Basierend auf X-Road hat Estland zudem den «Data Tracker» implementiert, welcher die Zugriffe auf Personendaten in ausgewählten Systemen aufzeichnet und den betroffenen natürlichen Personen zugänglich macht[120].

A.7.6. eDelivery (EU)

eDelivery ist analog zu X-Road zum Datenaustausch zwischen Systemen und über Landesgrenzen hinweg entwickelt worden[121]. eDelivery ist X-Road in vielen Aspekten sehr ähnlich, unterscheidet sich jedoch signifikant in folgenden zwei Punkten[122]:

- Sämtliche X-Road Komponenten sind Open-Source und müssen für die Implementierung eines X-Road Systems verwendet werden. eDelivery Komponenten müssen lediglich bestimmte Spezifikationen erfüllen, können selbst aber von einem beliebigen Hersteller erstellt werden und auch Closed-Source sein. Es kann bei eDelivery folglich beliebig viele Implementationen beispielsweise eines Access Points geben.
- Mitteilungen werden bei X-Road «synchron» ausgetauscht und bei eDelivery «asynchron». Je nach Anwendungsfall ergeben sich dadurch Vor- und Nachteile.

X-Road und eDelivery können somit auch komplementär eingesetzt werden: Estland verwendet beispielsweise beide Technologien[123].

---

[114] Siehe: https://www.hin.ch/

[115] Siehe: https://www.hin.ch/produkte/hin-praxispaket-plus/

[116] Siehe: https://x-road.global/xroad-history

[117] Siehe: https://x-road.global/

[118] Argentinien: https://x-road.global/integrity-and-interoperability-the-perfect-match-for-argentinas-public-service
Färöer Inseln: https://x-road.global/empowering-citizens-and-business
Island: https://x-road.global/iceland-joins-the-nordic-interoperability-league-with-straumurinn
El Salvador: https://x-road.global/first-steps-towards-interoperability-in-the-public-sector-of-el-salvador

[119] Siehe: https://x-road.global/case-study-the-business-registers-of-estonia-and-finland

[120] Siehe: https://e-estonia.com/data-tracker-build-citizen-trust/

[121] Siehe: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eDelivery

[122] Für weitere Unterschiede siehe auch: https://www.niis.org/blog/2019/9/26/x-road-and-edelivery-identical-twins-or-distant-relatives

A.8. Umsetzung der Nachvollziehbarkeitsfunktion in anderen Ländern

A.8.1. Dänemark

Dänemark gilt als eines der weltweit führenden Länder im Bereich von E-Government (siehe dazu beispielsweise das «E-Government Survey 2020» der UNO[124]). Dänemark bietet seinen Bürgern eine Vielzahl von elektronischen Dienstleistungen an wie beispielsweise die NemID (elektronische ID für die Identifizierung und die digitale Unterschrift), ein digitales Postfach für die Kommunikation mit der öffentlichen Verwaltung (Digital Post) sowie diverse Self-Service Leistungen (beispielsweise über das zentrale Verwaltungsportal «borger.dk» oder das zentrale Steuer-/Zollportal «skat.dk»). Eine Vielzahl von Aktivitäten, welche früher einen physischen Behördengang oder schriftlichen Postverkehr vorausgesetzt hatten, können heute 24/7 online von den Bürgern erledigt werden. Wichtig für die Umsetzung war und ist die Zusammenarbeit zwischen der Zentralregierung, den Regionen, den Gemeinden und auch mit privaten Akteuren [125].

Die Umsetzung der eGovernment Dienstleistungen findet in Dänemark in Zusammenarbeit zwischen der Zentralregierung, den Regionen[126] und Gemeinden statt. Für den Erfolg der Umsetzung sind in Dänemark drei Punkte wichtig:

1. Das Vertrauen der Bürger in die öffentliche Verwaltung darf unter Digitalisierungsprojekten nicht leiden. Im Gegensatz, die neuen Möglichkeiten müssen genutzt werden, um Bürgern einen leichteren Zugriff auf ihre Daten und einen besseren Überblick über die Nutzung der Daten zu geben. Die digitalen Möglichkeiten sollen zudem genutzt werden, um Bürgern die Möglichkeit zu geben, für spezifische Anwendungsfälle ihre Daten verwaltungsübergreifend zu teilen.
2. Die Digitalisierung soll dazu genutzt werden, die Angebote für die Bürger vereinfacht zu präsentieren: Es soll für den Bürger nicht mehr notwendig sein zu wissen, welche Verwaltungseinheit genau für seine Aufgabenstellung zuständig ist. Stattdessen müssen die Angebote themenbasiert für den Bürger an einer Stelle zusammengestellt sein.
3. Technologische Entwicklungen müssen frühzeitig geprüft und wenn sinnvoll umgesetzt werden.

Um die Transparenz der Datennutzung zu erhöhen, plant Dänemark die Einführung von «Mit Overblik» (Mein Überblick) über die nächsten Jahre als Teil des «borger.dk»-Portals (siehe Abbildung 22 und Abbildung 23). Mit dem Projekt werden folgende Ziele verfolgt:

- Überblick über alle offenen Vorgänge zwischen einer Person und der öffentlichen Verwaltung
- Ein digitales Postfach für sämtliche Kommunikation mit der öffentlichen Verwaltung
- Ein Kalender mit sämtlichen offenen Terminen (inklusive Reminder für nahende Deadlines)
- Übersicht darüber, welche Verwaltungseinheit auf die Informationen des Bürgers zugegriffen hat (analog zum bereits bestehenden Modell von «MinLog» auf dem Gesundheitsportal «sundhed.dk»). Diese Funktionalität ist aktuell in Planung und noch nicht operativ umgesetzt. Es ist zudem noch nicht abschliessend definiert, in welchem Umfang eine solche Funktionalität umgesetzt werden wird[127]. Dieser geplante Teil von «Mit Overblik» entspricht in etwa dem mit UZ13 verfolgten Ziel.

---

[123] Siehe: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/2019/07/17/Estonia+sets+an+example+in+e-invoicing

[124] Details siehe https://www.egovernment.ch/index.php/download_file/1784/3343/

[125] Weitere Details siehe bspw. https://en.digst.dk/media/18772/world-class-digital-service.pdf

[126] In Dänemark haben Regionen weniger Befugnisse als Kantone in der Schweiz.

[127] Quelle: https://en.digst.dk/media/18772/world-class-digital-service.pdf

Abbildung 22: "Mit Overblick" als zentrales Portal für Dänische Bürger[128]

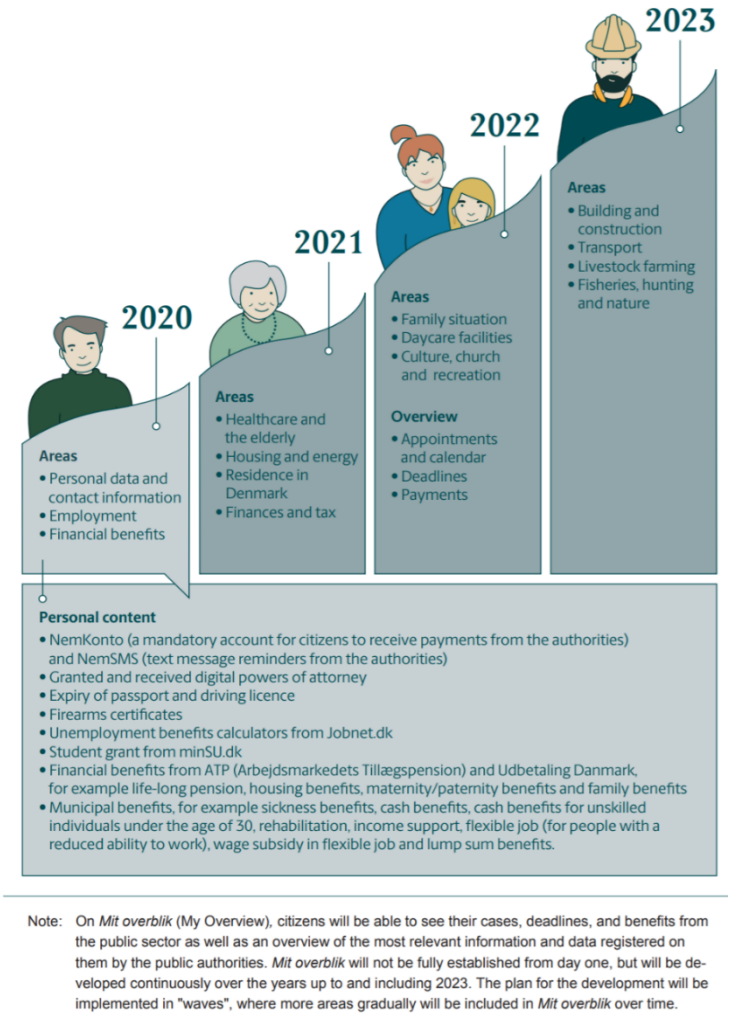

Abbildung 23: Implementierungsroadmap für "Mit Overblik"[128]

[128] Quelle: https://en.digst.dk/media/18772/world-class-digital-service.pdf

A.8.2. Estland

Estland hat seit 2017 den «Data Tracker» im Einsatz[129]. Jeder Bürger mit einer elektronischen Identität kann auf diesem Portal (eesti.ee) die vollständige Liste an Datenzugriffen von Verwaltungseinheiten auf die aktuell folgenden vier[130] am Data Tracker angeschlossen nationalen IT-Systeme einsehen:

- Das Einwohnerregister
- Die Krankenversicherung
- Die Arbeitslosenversicherung
- Die Sozialversicherung

Die Bürgerinnen und Bürger können sehen, wann welche Einrichtung auf ihre Daten zugegriffen hat. Eine Verlinkung der Datenzugriffe mit «Events im realen Leben» ist geplant aber aktuell noch nicht umgesetzt.

«My Tracker» ist Teil der nationalen Datenaustausch-Architektur «X-Road»[131]. Über die oben genannten vier angeschlossenen Datenbanken werden über die «X-Road» Architektur jährlich ca. 35 Millionen Abfragen bearbeitet (bei ca. 1 Million Einwohnern). Zur IT-Architektur in Estland gehört ebenfalls eine nationale elektronische Identität, welche als Grundlage für die digitale Kommunikation mit der öffentlichen Verwaltung dient. Die digitale Daten-Architektur von Estland beruht auf den Prinzipien der Tallinn Declaration on eGovernment, siehe Abschnitt 4.4. Estland verfolgt einen stark zentralisierten Ansatz[132].

A.8.3. Luxemburg

Bürger in Luxemburg können auf «MyGuichet.lu» elektronisch sämtliche über sie gespeicherte Informationen aus dem Personenregister[133] anzeigen lassen. Zudem besteht die Möglichkeit, sämtliche Datenzugriffe der letzten 6 Monate anzuzeigen. Mittels Brief-Template können die Bürger im Zweifel den Grund des Datenzugriffs erfragen. Es können auch Freigaben für die Datenverwendung durchgeführt werden: Entweder fallweise oder für eine zuständige Stelle.

Luxemburg ist ähnlich wie die Schweiz in Kantone und Gemeinden unterteilt[134]. Auf «MyGuichet.lu» können denn auch die Gemeinden ihre Dienstleistungen anbieten – beispielsweise die Registrierung zur Briefwahl[135].

---

[129] Details siehe auch: https://e-estonia.com/data-tracker-build-citizen-trust/

[130] Mit dem «Data Tracker» können nicht die Zugriffe auf alle an X-Road angeschlossenen IT-Systeme eingesehen werden, sondern lediglich die vier oben genannten.

[131] Siehe auch Abschnitt A.7.5

[132] Siehe auch zur Geschichte von X-Road: https://x-road.global/xroad-history

[133] «Nationales Register natürlicher Personen und Identifizierung natürlicher Personen»

[134] Wobei Kantone in Luxemburg deutlich weniger Befugnisse haben, als Kantone in der Schweiz.

[135] Siehe: https://guichet.public.lu/de/actualites/2021/fevrier/01-vote-correspondance-sandweiler.html

A.9. Anforderungen an die Aggregation und Aufbereitung von Daten

A.9.1. Aufbereiten und Aggregieren von Daten

Die in den Quellsystemen gespeicherten Rohdaten werden in vielen Fällen für natürliche Personen nicht ausreichend verständlich sein. Dies gilt sowohl für die Personendaten als auch die Metadaten. Folgende zwei fiktive Beispiele zeigen dies für den Fall auf, dass einer natürlichen Person sowohl Einsicht in die Daten selbst als auch in die Zugriffsinformationen gegeben wird.

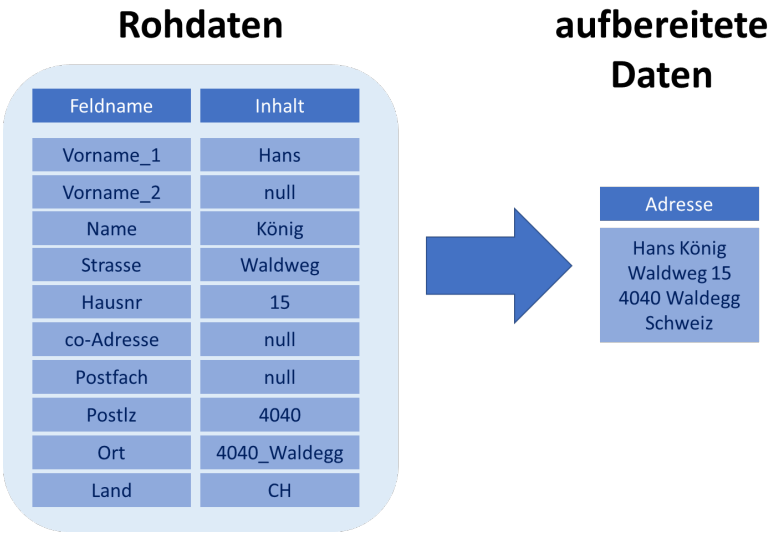

Abbildung 24: Aufbereitung von Rohdaten (fiktives Beispiel)

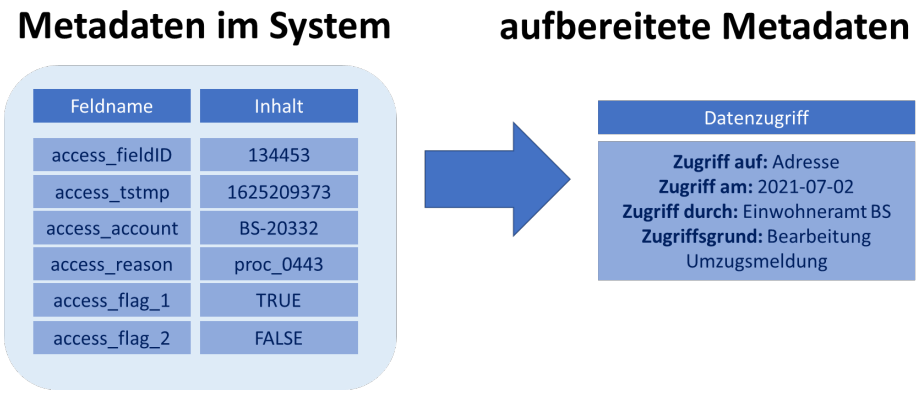

Abbildung 25: Aufbereitung von Metadaten (fiktives Beispiel)

Um die Daten für die Nutzenden der Nachvollziehbarkeitslösung verständlich aufzubereiten, sind verschiedene Massnahmen notwendig. Folgende Liste zeigt exemplarisch eine Auswahl von möglichen Datentransformationen:

- Feldnamen in verständliche Beschreibungstexte übersetzen
- Technische Werte (bspw. Zeitstempel, Ländercodes, …) in für Menschen lesbare Werte (bspw. Datum) übersetzen
- Daten aus verschiedenen Feldern aggregieren
- Daten weglassen (bspw. technische Felder eines Quellsystems oder Felder ohne Inhalt)
- Aussagekräftige Beschreibungstexte der Daten als Erklärung mitliefern.

Da für die Aufbereitung der Daten spezifisches fachliches Wissen notwendig ist, muss diese Übersetzung idealerweise beim Export der Daten aus dem entsprechenden Quellsystem durchgeführt werden.

Neben der Verständlichkeit der Daten für natürliche Personen muss auch darauf geachtet werden, dass die Daten für natürliche Personen relevant sind und die richtige Flughöhe gewählt wird. Greift beispielsweise die Steuerbehörde auf das Steuerdossier 2021 einer natürlichen Person zu, so macht es wenig Sinn, der entsprechenden natürlichen Person mehrere Dutzende separate Zugriffe auf einzelne Datenfelder auszuweisen. Eine sinnvolle Aggregation auf einzelne Themengebiete (bspw. «Zugriff auf Vermögensverzeichnis Steuererklärung 2021») oder sogar das ganze Dossier («Zugriff auf Steuerdossier 2021») können hier zielführend sein.

A.9.2. Standardisierung und Harmonisierung, eindeutige Identifikatoren

Um Daten für natürliche Personen verständlich aufzubereiten, kann es notwendig sein, diese über verschiedene Quellsysteme hinweg zu aggregieren, wie das fiktive Beispiel[136] in Abbildung 26 zeigt.

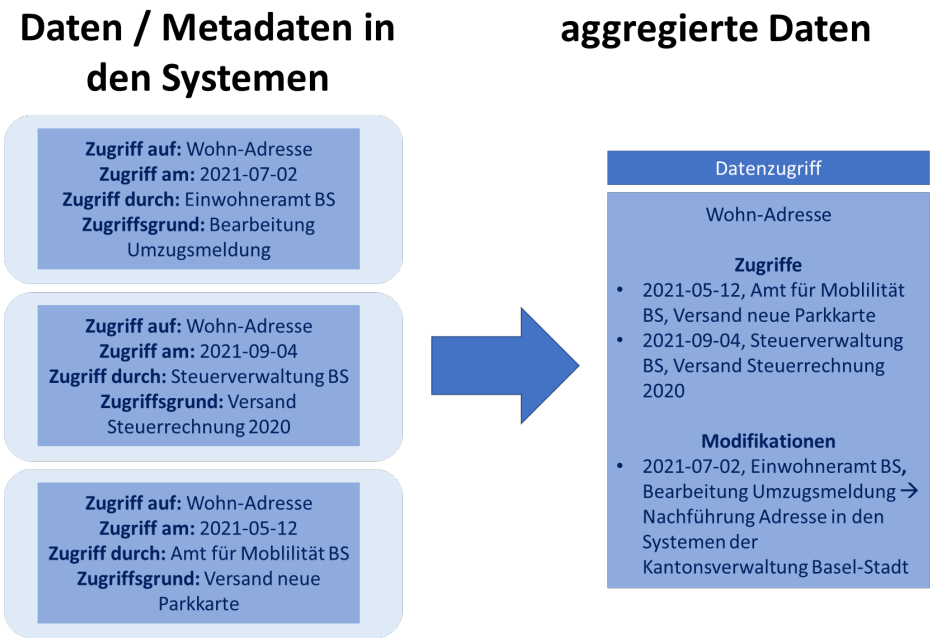

Abbildung 26: Aggregation von Daten über Quellsysteme hinweg (fiktives Beispiel)

Werden ähnliche Daten aus verschiedenen Systemen für eine natürliche Person nicht harmonisiert dargestellt, so ist es für diese schwierig, über diese die Übersicht zu behalten. Eine Aggregation von Daten über verschiedene Quellsysteme stellt verschiedene Anforderungen an die gespeicherten Daten:

- Daten aus verschiedenen Quellsystemen müssen eindeutig einer natürlichen Person zugeordnet werden können. Eindeutige und einheitliche Identifikatoren helfen dabei.
- Daten müssen standardisiert und harmonisiert sein: Ansonsten ist ein Zusammenzug und einer harmonisierte Darstellung von ähnlichen oder gleichen Daten aus verschiedenen Quellsystemen stark erschwert (im Beispiel exemplarisch dargestellt, indem alle Adressen als «Wohnadresse» und nicht beispielsweise als «Rechnungsadresse» gespeichert sind).

[136] Dieses Beispiel dient nur der Illustration des Sachverhaltes und soll nicht als Empfehlung für eine bestimmte Art der Darstellung / Aggregation verstanden werden.

A.9.3. Datenqualität

Die in den Quellsystemen vorhandenen Daten und Metadaten sollten gewisse Mindeststandards bezüglich der Datenqualität erfüllen:

- Die Daten müssen zuverlässig und eindeutig einer natürlichen Person zugeordnet werden können – sowohl innerhalb des Systems als auch über Systemgrenzen hinweg. Ansonsten besteht die Gefahr, dass eine unberechtigte Person Einsicht in Personendaten einer anderen Person erhält und dadurch die Anforderungen des Datenschutzes nicht erfüllt würden.
- Die Metadaten, welche die Zugriffe der öffentlichen Verwaltung auf die Daten protokollieren, müssen lückenlos und fehlerfrei erfasst werden, da ansonsten den natürlichen Personen falsche bzw. unvollständige Auskünfte erteilt werden, was das Vertrauen in die öffentliche Verwaltung beschädigen würde.
- Falls den natürlichen Personen Daten angezeigt werden, sollten diese grösstenteils korrekt und aktuell sein. Häufige Fehler würden das Vertrauen in die Arbeit der Verwaltung beschädigen.

Nur wenn diese Mindestanforderungen erfüllt sind, eignet sich ein Quellsystem für eine Anbindung an eine Nachvollziehbarkeitslösung.

A.10. Anforderungen an anzuschliessende Quellsysteme

A.10.1. «Level» der Nachvollziehbarkeit definieren

Jedes potenziell an eine Nachvollziehbarkeitslösung anzuschliessende Quellsystem ist anders. Während gewisse Quellsysteme pro natürlicher Person nur relativ wenige und gut verständliche Daten gespeichert haben, sind in anderen Quellsystemen komplexe Dossiers mit möglicherweise vielen angehängten Dokumenten vorhanden. Folgende zwei Beispiele illustrieren dies anhand der Anwendungsfälle «Wer hat meine Daten genutzt?»:

- Das UPI-Register speichert lediglich wenige Attribute über natürliche Personen, welche grösstenteils selbsterklärend sind: Name und Vorname der Person, Geschlecht, Geburtsdatum, Nationalität sowie die AHV-Nummer[137].
- Das System einer kantonalen Steuerverwaltung enthält sämtliche Informationen, welche bei einer Steuererklärung mitgeliefert werden. Für jedes Steuerjahr entsteht so ein Falldossier mit verschiedenen Beilagen. Weiter sind noch diverse interne Prozessinformationen gespeichert.

Im ersten Beispiel reicht es vermutlich, wenn im Rahmen der Nachvollziehbarkeitslösung die Information zur Verfügung gestellt wird, dass auf den Datensatz (i.e. Gesamtheit der gespeicherten Informationen) der Person zugegriffen wurde. Zudem sollte der Zugriffszeitpunkt, die zugreifende Organisationseinheit und der Zugriffsgrund dokumentiert werden. Grundsätzlich könnte auch der Inhalt der gespeicherten Daten zur Verfügung gestellt werden.

Im zweiten Beispiel ist die Ausgangslage weniger eindeutig. Welche Granularität an Informationen sollte der natürlichen Person zur Verfügung gestellt werden?

- Zugriff auf den Datensatz (i.e. eine beliebige Information aus einem beliebigen Steuerdossier)?
- Zugriff auf das Steuerdossier des Jahres X?
- Zugriff auf einzelne Formulare und Belege der Steuererklärung des Jahres X?
- Zugriff auf einzelne Ziffern der Steuererklärung des Jahres X?
- Zugriff auf einzelne Felder in der Datenbank?

Bei der Entscheidung darüber, auf welchem «Level» die Informationen aggregiert werden sollen, müssen verschiedene Fragestellungen berücksichtigt werden. Einige sind exemplarisch aufgeführt:

- Versteht die natürliche Person die bereitgestellte Information?
- Findet die natürliche Person die Information, welche sie erwartet?
- Darf die entsprechende Information der natürlichen Person angezeigt werden (insbesondere bei internen Prozessinformationen) oder gibt es rechtliche Grundlagen, welche dies verbieten?

Zusammengefasst muss entschieden werden, welcher «Use-Case» der Nachvollziehbarkeit umgesetzt werden soll: Welche Information braucht die natürliche Person vom jeweiligen Quellsystem, um grösstmögliche Transparenz und Vertrauen zu schaffen?

[137] Optional sind manchmal noch der Ledigname, die Namen der Eltern, das Geburtsland sowie der Geburtsort gespeichert.

Es besteht zudem die Möglichkeit, einer natürlichen Person mehrere Ansichten der Informationen zur Verfügung zu stellen: Möchte die natürliche Person zusätzliche Informationen, könnten per Knopfdruck zusätzliche Details angezeigt werden.

Soll eine skalierbare Nachvollziehbarkeitslösung aufgebaut werden, kann die Definition von einigen generischen Use-Cases hilfreich sein, an welchen sich verschiedene Quellsysteme orientieren können. So kann der natürlichen Person die von verschiedenen Quellsystemen bereitgestellte Information immer in ähnlicher Art und Weise präsentiert werden.

A.10.2. Anforderungen an das Logging der Zugriffe im Quellsystem

Je nach gewählter Lösungsvariante müssen andere Informationen im Quellsystem erfasst werden. Im Falle der Variante «Wer hat meine Daten genutzt» müssen folgende Bedingungen erfüllt sein:

- Jedes gespeicherte Personendatum muss mit dem eindeutigen Identifikator der betreffenden natürlichen Person verlinkt sein.
- Jeder Zugriff auf ein Datum oder einen aggregierten Datensatz (siehe vorhergehender Abschnitt) muss geloggt werden. Folgende Liste illustriert beispielhaft, welche Informationen dabei erfasst werden könnten:
    - Auf welche Daten wurde zugegriffen?
    - Zeit und Datum des Zugriffs.
    - Account, von welchem zugegriffen wurde inkl. eindeutiger Zuordnung zu der Organisationseinheit, zu welcher der Account gehört.
    - Art des Zugriffs
        - Einsicht oder Bearbeitung der Daten durch eine Person
        - Bearbeitung der Daten durch das Quellsystem selbst (bspw. zur Erstellung eines Reports / einer Statistik)
        - Einsicht oder Bearbeitung von Daten durch ein Drittsystem
        - Datenweitergabe von nicht anonymisierten Daten an ein Drittsystem
    - Aktion auf oder Verwendung der Daten (Erfassen, Einsicht, Mutation, Löschen)
    - Grund für den Zugriff (siehe nächster Abschnitt)

Für gewisse Zugriffe ist sicherzustellen, dass diese der natürlichen Person nicht angezeigt werden oder alternativ gar nicht erst geloggt werden. Dies ist dann der Fall, wenn rechtliche Rahmenbedingungen dies nicht erlauben[138]. Weiter ist die Aufbewahrungsfrist für diese Log-Daten zu definieren.

Unabhängig davon gibt es noch weitere Faktoren, welche beim Logging der Zugriffe (respektive derer Aggregation) berücksichtigt werden können:

- Können / sollen gezielte Einzelzugriffe von Zufallstreffern über eine Suchfunktion unterschieden werden?
- Sollen Zugriffe über eine Schnittstelle von Zugriffen über eine Benutzeroberfläche unterschieden werden?

[138] Ein Beispiel wären Zugriffe im Rahmen von laufenden Ermittlungsverfahren

- Sind kurzzeitig hintereinander folgende Zugriffe der gleichen Person mit dem gleichen Grund zu aggregieren?
- Ist eine unterschiedliche Aggregation für Zugriffe des Eigentümers der Datensammlung und von Drittparteien sinnvoll?

A.10.3. Grund des Zugriffs

Wird im Rahmen einer Lösungsvariante «Wer hat meine Daten genutzt» die Aussage gegenüber einer natürlichen Person gemacht, dass auf bestimmte Daten zugegriffen wurde, so sollte zur Förderung der Transparenz auch ein Grund für den Zugriff mitgeteilt werden. Exemplarisch sind einige Möglichkeiten aufgeführt:

- Auswahl eines oder mehrerer Gründe aus einem vordefinierten Katalog
- Name des Verwaltungsprozesses oder der Verwaltungsleistung, basierend auf welcher zugegriffen wurde
- präzise Angabe der Rechtsgrundlage, sofern sich dadurch für die nat. Person der Verwendungsgrund ableiten lässt
- ein beliebiger Freitext
- Die einmalige Angabe des Grundes / der Gründe, basierend auf welchen ein User auf die Daten zugreifen kann. Bei jedem Zugriff dieses Users wird dann der gleiche Grund / die gleichen Gründe angegeben.

Verschiedene Ansätze haben verschiedene Vor- und Nachteile. Der Nutzen für die natürliche Person muss dem zusätzlichen Aufwand und der Komplexität auf Seite der Verwaltung gegenübergestellt werden: Ein gut verfasster Freitext kann beispielsweise genaue Informationen liefern, weshalb auf Personendaten der natürlichen Person zugegriffen wurde. Der Freitext erzeugt aber einen grossen Mehraufwand im Rahmen der Prozesse der Verwaltung und die Qualität des Textes hängt stark von der jeweiligen Person ab, welche diesen verfasst. Es wird daher empfohlen eine Variante zu wählen, welche sich grösstmöglich automatisieren lässt. Dies bedingt, dass ein Katalog von Gründen geführt wird. So kann der Zusatzaufwand für die Verwaltung klein gehalten und dadurch die Akzeptanz für die Nachvollziehbarkeitslösung gefördert werden.

A.11. Rahmenbedingungen für die Architektur einer Nachvollziehbarkeitslösung

A.11.1. Zentral vs. Föderiert vs. Dezentral

Es gibt drei fundamental unterschiedliche Architekturvarianten sowie beliebig viele Mischformen davon:

- **Zentral**: Es gibt ein zentrales Nachvollziehbarkeitssystem, an welchem sämtliche Quellsysteme angeschlossen sind. Ein Beispiel für eine solche Umsetzung ist das System von Estland. Eine natürliche Person kann sich auf einem zentralen Nachvollziehbarkeits-Portal einloggen und Daten sämtlicher angeschlossener Systeme einsehen.
- **Föderiert**: Es gibt mehrere dezentrale Nachvollziehbarkeitssysteme, welche miteinander verbunden sind. So könnte es beispielsweise für den Bund und für jeden Kanton ein eigenes Nachvollziehbarkeitssystem geben. Föderiert bedeutet in diesem Zusammenhang, dass sich eine natürliche Person auf dem Nachvollziehbarkeitsportal des Wohnkantons einloggen kann und über dieses neben den Daten des kantonalen Nachvollziehbarkeitssystems auch die Daten des Nachvollziehbarkeitssystems des Bundes und der Nachvollziehbarkeitssysteme der anderen Kantone angezeigt bekommt.
- **Dezentral**: Bei einem dezentralen Ansatz gibt es verschiedenen nicht miteinander verbundene Systeme zur Nachvollziehbarkeit. Der Grad der Dezentralisierung kann variieren: Von einem kantonalen Nachvollziehbarkeitssystem bis hin zu einer separaten Weboberfläche für den Zuriff auf die Informationen pro Quellsystem sind beliebige Varianten denkbar.

Aus Sicht der natürlichen Personen ist eine zentrale oder eine föderierte Lösung zu bevorzugen, da mit diesen Ansätzen Zugriff auf sämtliche Informationen an einer zentralen Stelle möglich wird. Die politische Umsetzbarkeit dürfte bei einem föderierten Nachvollziehbarkeitssystem besser sein als bei einem zentralisierten Ansatz (siehe auch Abschnitt 6.5).

A.11.2. Aufgabenteilung zwischen Quellsystemen, Backend(s) und Benutzeroberflächen(s)

Eine Nachvollziehbarkeitslösung wird aus verschiedensten Komponenten bestehen. Im Rahmen der Architekturdefinition muss das Zusammenspiel sowie die Aufgabenteilung der verschiedenen beteiligten Komponenten definiert werden.

A.11.3. Schnittstellen und Standards

Im Rahmen der Architekturdefinition müssen auch Schnittstellen und Standards definiert werden. Im Folgenden je ein Beispiel:

- **Schnittstellen**: Die Schnittstellen regeln den Datenaustausch zwischen den jeweiligen angeschlossenen Quellsystemen und der Nachvollziehbarkeitslösung. Eine einheitliche Schnittstellendefinition reduziert die Komplexität bei der Implementierung der Nachvollziehbarkeitslösung.
- **Standards**: Die von den Schnittstellen übertragenen Daten sollten standardisiert sein, um den Nutzenden eine einheitliche Sicht zu bieten sowie eine nachgelagerte Aggregation von Daten verschiedener Quellsysteme zu ermöglichen.

A.11.4. Technologieneutralität als anzustrebender Zustand für längerfristige Lösung

Der Aufbau einer Nachvollziehbarkeitslösung ist ein langfristiges Vorhaben. Die Architektur sollte daher so gewählt werden, dass diese nicht allzu stark von einer einzelnen Technologie abhängig ist, welche mit der Zeit veralten kann[139].

A.11.5. Push vs. Pull

Es gibt zwei grundsätzlich unterschiedliche Ansätze für den Datenaustausch zwischen den angeschlossenen Quellsystemen und der Nachvollziehbarkeitslösung:

- Push: Die Quellsysteme melden jeden Zugriff an die Nachvollziehbarkeitslösung.
- Pull: Die Nachvollziehbarkeitslösung fragt bei Bedarf bei den angeschlossenen Quellsystemen an.

Die Umsetzung der Push-Funktion bedeutet, dass die Nachvollziehbarkeitslösung Daten auf Vorrat speichern muss. Dieses Datenspeichern auf Vorrat könnte bei Politik und Bevölkerung auf Widerstand stossen (siehe auch Abschnitt 6.5).

A.11.6. Der Datenschutz und die Datensicherheit als Schlüsselanforderungen

Die Umsetzung einer Nachvollziehbarkeitslösung darf nicht dazu führen, dass dadurch der Datenschutz oder die Datensicherheit geschwächt werden (siehe auch Abschnitt 6.5). Folgende Punkte sind dabei mindestens zu beachten:

- Informationen über die Verwendung der Personendaten durch die öffentliche Verwaltung sind «Metadaten» zu den betreffenden Personendaten. Selbst ohne den Inhalt der Personendaten zu kennen, lassen sich aus diesen Metadaten Rückschlüsse über die betreffenden natürlichen Personen ableiten: Das Strassenverkehrsamt hat auf die Adresse zugegriffen? Die Person besitzt vermutlich ein Auto oder Motorrad. Das Betreibungsregisteramt hat auf die Adresse einer Person zugegriffen? Es könnte eine Betreibung hängig sein. Diese Metadaten sind daher vor unberechtigtem Zugriff gleich wie Personendaten zu schützen.
- Je mehr solcher Metadaten und gegebenenfalls sogar die dazugehörigen Personendaten über einen Zugangspunkt zugreifbar sind, desto interessanter wird dieses Ziel für Cyberkriminelle. Entsprechende Schutzmassnahmen auf der Systemseite als auch auf der Nutzerseite (bspw. Mehrfaktor-Authentifizierung) sind zwingend umzusetzen. Benachrichtigungen der natürlichen Person per Email / SMS / … bei Zugriff auf die entsprechenden Daten der Nachvollziehbarkeitslösung sind eine gute Möglichkeit, hier zusätzliche Transparenz zu schaffen.

Die gewählte Architektur muss diese Aspekte zwingend berücksichtigen.

A.11.7. Durch Authentifizierung unbefugte Zugriffe verhindern

Der eCH-Standard eCH-0170[140] definiert vier verschiedene Vertrauensstufen für die Authentifizierung von (natürlichen) Personen. Da bei der Nachvollziehbarkeitslösung schützenswerte (oder ggf. besonders schützenswerte) Personendaten betroffen sind, ist mindestens Level 3 «beträchtliches Vertrauen» umzusetzen. Stufen eins («kein oder minimales Vertrauen») sowie zwei («geringes Vertrauen») sind nicht ausreichend. Eine national anerkannte E-ID dürfte diese Anforderung von «Level 3» erfüllen.

---

[139] Die Verwendung von APIs und Microservices bietet eine Möglichkeit, dies zu erreichen.

[140] https://www.ech.ch/de/standards/60593

Zugriffe durch natürliche Personen auf die Nachvollziehbarkeitslösung sind zu loggen. Es ist zudem zu prüfen, ob eine Push-Nachricht (bspw. SMS, Email) bei Login-Versuchen (erfolgreich oder nicht erfolgreich) an die natürliche Person gesendet werden soll.

A.11.8. Benutzeroberfläche

Eine Nachvollziehbarkeitslösung braucht zwingend eine Benutzeroberfläche[141], auf welche die Informationen zur Verwendung der eigenen Personendaten den natürlichen Personen präsentiert werden. Die Gestaltung dieser Oberfläche soll sich an den Anforderungen der natürlichen Personen orientieren (siehe Abschnitt 6.3.1).

Aus Sicht der Nutzenden ist es wünschenswert, wenn die Nachvollziehbarkeitslösung möglichst nahtlos in bestehende Portale (bspw. aus den Kantonen) eingebunden werden kann. Dies senkt die Hürde, um die bereitgestellten Informationen einzusehen: «Ich habe gerade meine Steuererklärung eingereicht und bin sowieso eingeloggt: Da kann ich doch gleich noch schauen, was mit meinen letztjährigen Steuerdaten alles passiert ist.»

[141] Eine analoge Lösung, wie sie heute für das Auskunftsbegehren gemäss Datenschutzgesetz umgesetzt wird, ist heute nicht mehr zielführend: Einerseits aufgrund des grossen Aufwands für die öffentliche Verwaltung und andererseits aufgrund der Erwartungshaltung nach digitalen Lösungen durch die Bevölkerung.

A.12. Projekte, Initiativen, Produkte und Lösungen mit möglichem Einfluss auf UZ13 Nachvollziehbarkeitslösung

Es gibt eine Vielzahl von Initiativen und Projekten, welche für UZ13 Nachvollziehbarkeitslösung relevant sein könnten. Diese Auswahl ist exemplarisch und erhebt keinen Anspruch auf Vollständigkeit.

A.12.1. Aktivitäten basierend auf den Umsetzungszielen des «Umsetzungsplans 2021-2023 E-Government Schweiz»

Tabelle 9 listet die Umsetzungsziele des «Umsetzungsplans 2021-2023 E-Government Schweiz» auf, welche möglicherweise Synergien oder Abhängigkeiten mit UZ13 haben.

Tabelle 9: Umsetzungsziele des «Umsetzungsplans 2021-2023 E-Government Schweiz» mit potenzieller Relevanz für UZ13

Umsetzungsziel[142]	Relevanz für UZ13
UZ1: EasyGov.swiss ausbauen	Fokus auf juristische Personen. Braucht für die Identifikation und Rollenzuteilung Daten von natürlichen Personen.
UZ2: eUmzugCH schweizweit ausbreiten	Bereits heute in vielen Kantonen eingesetzt für Umzugsmeldungen (Abmeldung alter Wohnort, Anmeldung neuer Wohnort). Enthält Personendaten und dadurch für UZ13 potenziell interessant. Sedex wird als Bussystem verwendet.
xUZ3: E-Voting neu ausrichten und stabilen Versuchsbetrieb sicherstellen	Bei einer möglichen zukünftigen Umsetzung als potenziell anzuschliessendes System für UZ13 relevant.
UZ4: Signaturvalidator schweizweit etablieren	Validierung von elektronisch signierten Behördendokumenten und folglich für UZ13 nicht relevant.
UZ5: E-Partizipationsprojekte auf kommunaler und kantonaler Ebene fördern	Aktuell unklar, ob daraus für UZ13 relevante Systeme entstehen.
UZ6: Nutzerfreundlichkeit der elektronischen Behördenleistungen verbessern	Die durch das UZ6 erarbeiteten Guidelines und Regeln für eine verbesserte Nutzerfreundlichkeit sind bei einer allfälligen Umsetzung von UZ13 zu berücksichtigen.
UZ7: Behördenübergreifende E-Information und Betrieb des neuen ch.ch etablieren	Zentrales Portal zur Information der Bevölkerung durch die Behörden und somit für UZ13 nicht relevant.
UZ8: E-ID umsetzen	Könnte als Identifikator für ein Nachvollziehbarkeitslösung verwendet werden (analog zu bspw. Estland)
UZ9: Behördenübergreifende Stammdatenverwaltung aufbauen	Für das Projekt relevant, diverse Register mit Personendaten sind im Projektscope enthalten: • Betriebs- und Unternehmensregister (BUR, UID) • Gebäude- und Wohnungsregister (GWR) • Gemeinde und kantonale Einwohnerregister (EWR) via Nationaler Adressdienst (NAD) Erarbeitung eines nationalen Stammdatenmodells sowie der dazugehörigen Governance. Etablierung einer «Nationale Dateninfrastruktur».
UZ10: Nationaler Adressdienst aufbauen	Für das Projekt relevant, da ein neues nationales Adressregister zum Abgleich von Adressdaten von (natürlichen) Personen aufgebaut werden soll[143]. Als zentrales System der Adressverwaltung für UZ13 als mögliches Quellsystem relevant.
UZ11: Anonymisierte und nicht vertrauliche Daten von Bund, Kantonen und Gemeinden frei zugänglich machen (Open Government Data)	Für UZ13 nicht relevant (betrifft keine Personendaten).
UZ12: Standardisierung fördern	Hierbei geht es um die Förderung von eCH-Standards, welche bei einer allfälligen Umsetzung von UZ13 relevant

[142] Siehe: https://www.egovernment.ch/files/5815/8039/0240/Umsetzungsplan_2020_D.pdf

[143] Siehe: https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-76062.html

	werden.
UZ14: E-Government-Architektur für den strategischen Umsetzungsplan erarbeiten und führen	Für UZ13 relevant, da Architekturentscheidungen zur Umsetzung von UZ13 mit der übergreifenden Architektur aus UZ14 abgestimmt werden müssen. Als Teil von UZ14 wird aktuell auch noch das Teilprojekt «DataHub4Gov» betrachtet.
UZ15: Projekte der Gemeinwesen in den Bereichen Informatik und E-Government unterstützen	Nicht relevant
UZ16: Innovative Projekte fördern	Gegebenenfalls sind Projekte relevant, welche aus UZ16 heraus entstehen.
UZ17: Datenplattformen der Verwaltung fördern	Da es um die Beschaffung von neuen Datenplattformen geht, könnten Anforderungen von UZ13 hier ggf. zu einem späteren Zeitpunkt platziert werden.
UZ18: Beratung und Koordination in rechtlichen Fragen anbieten	Hier bietet sich für UZ13 ggf. die Möglichkeit, rechtliche Abklärungen durchzuführen.
UZ19: Vertrauen der Bevölkerung und Wirtschaft in die elektronischen Behördenleistungen stärken	Hier bietet sich für UZ13 ggf. die Möglichkeit, die Öffentlichkeit über das Projekt zu informieren.

A.12.2. Projekt «Interoperatibilitätsplattform (IOP)» als Umsetzung des Bundesratsauftrags «Nationale Datenbewirtschaftung (NaDB)»

Damit Daten ausgetauscht werden können, muss deren Interoperabilität sichergestellt werden. Das dazu bezüglich der Daten notwendige gemeinsame Verständnis wird durch deren Strukturierung und Standardisierung sowie durch Transparenz erreicht. In einem mit den notwendigen Instrumenten ausgestalteten interoperablen System können diese Informationen für alle beteiligten Stellen einsehbar und nutzbar gemacht werden. Damit wird gewährleistet, dass langfristig eine Übersicht aller beim Bund verfügbaren Daten besteht. Die effektiven Dateninhalte werden wie bisher in den lokalen Datensammlungen in der Verantwortung der jeweiligen Verwaltungsstellen gehalten.

Das Projekt Interoperabilitätsplattform (IOP) verfolgt folgende Arbeitsziele:

- Initiieren einer Interdepartementalen Arbeitsgruppe für das Programm NaDB (IDA-NaDB). Das Gremium soll aus Vertretern aller Departemente bestehen und ist für die Standardisierung, Normierung und Harmonisierung verantwortlich.
- Definition der Ablauf- und Aufbauorganisation zur Erstellung einer Interoperabilitäts-Stelle (IOS) beim BFS, welche operativ die IDA-NaDB unterstützt und deren Aufträge umsetzt.
- Definition und Koordination der Standardisierungs- und Harmonisierungsprozesse zur Gewährleistung der Interoperabilität in der Schweiz.
- Aufbau einer technischen Interoperabilitätsplattform (IOP) als Werkzeug und Instrument für die Standardisierung und Harmonisierung der Daten sowie zur Führung und Publikation der Standards und der gemeinsamen Modellierung von Metadaten dient.
- Definition der Ablauf- und Aufbauorganisation des Betriebs der technischen Interoperabilitätsplattform (IOP)

Das Eidgenössische Departement des Inneren EDI wurde beauftragt, ein interdepartementales Gremium zum Aufbau und zur Führung der Interoperabilitäts-Plattform (IOP) einzusetzen. Das Gremium wird durch eine beim EDI bzw. beim Bundesamt für Statistik (BFS) neu aufzubauende Interoperabilitätsstelle (IOS) operativ unterstützt. Das EDI wird in Abstimmung mit den anderen Departementen sowie bestehenden interdepartementalen Koordinationsorganen (z.B. Steuerungsgremium gemeinsame Stammdatenverwaltung Bund, Koordinationsorgan des Bundes für Geoin-

formation, usw.) die Prozesse, Rollen und Verantwortlichkeiten zur Führung und Steuerung festlegen. [144]

Relevanz für UZ13: Der aus dem Projekt IOP entstehende Datenkatalog kann mittelfristig dafür genutzt werden, weitere IT-Systeme mit relevanten Personendaten zu identifizieren. Die definierten Metadatenmodelle sollten bei der Umsetzung von UZ13 zur Anwendung kommen. Gegebenenfalls besteht die Option, einen Teil der Infrastruktur mitzunutzen.

A.12.3. ePortal vom EFD

Das ePortal[145] vom Eidgenössischen Finanzdepartement (EFD) bietet verschiedene Dienstleistungen an. Die aktuell angebotenen Dienstleistungen, welche Personendaten beinhalten, betreffen nur eine verhältnismässig kleine Anzahl von natürlichen Personen.

A.12.4. easygov.swiss

Easygov.swiss[146] ist der «Online-Schalter für Unternehmen». Die angebotenen Dienstleistungen richten sich denn auch ausschliesslich an Unternehmen: Anmeldung der MWSt., Anmeldung bei AHV/IV, Eintrag im Handelsregister etc. Easygov.swiss speichert aktuell wenige Personendaten (bspw. im Bereich der User-Profile). Beispielsweise im Bereich der AHV/IV fliessen über die Plattform allerdings Personendaten, welche dann in den entsprechenden Systemen gespeichert werden.

A.12.5. Online-Dienste

Die Website https://online-services.admin.ch/de listet verschiedenste Online-Dienste von Bund und Kantonen auf. Das Zielpublikum sind kleine und mittlere Unternehmen. Einzelne der aufgelisteten Dienstleistungen sind jedoch auch für natürliche Personen relevant.

A.12.6. eGovernment UVEK

Im Jahr 2017 hat das UVEK beschlossen, ein eigenes «eGovernment-Portal UVEK» aufzubauen[147]. In einem ersten Schritt werden Prozesse rund um das Thema «Abfall und Rohstoffe» auf dem Portal aufgeschaltet, sodass die heute dafür verwendete Applikation «veva-online» abgeschaltet werden kann. Es ist davon auszugehen, dass diese Plattform für UZ13 relevant werden könnte.

A.12.7. Projekt «Trusted Data Hub» der Schweizerischen Post

Dieses Vorhaben der Schweizerischen Post ist aktuell in einem sehr frühen Stadium – es sind nur wenige Details[148] bekannt. «Ziel sei es, Daten sicher, unveränderbar sowie nachvollziehbar zu transportieren und zu gewährleisten, dass Absender und Empfänger berechtigt seien, die jeweiligen Informationen zu erhalten und zu versenden.»

Für UZ13 ist das Projekt im aktuellen Status nicht relevant.

---

[144] Der Text in diesem Abschnitt wurde in gekürzter und redigierter Form aus einem Studienentwurf des IOP-Projektes entnommen (Stand Ende September 2020). Der finale Studientext kann von dieser Version abweichen.

[145] Siehe: https://eportal.admin.ch/start

[146] Siehe: https://www.easygov.swiss/easygov/#/de

[147] Siehe: https://www.bafu.admin.ch/bafu/de/home/themen/abfall/fachinformationen/abfallpolitik-und-massnahmen/portal-abfall-rohstoffe.html

[148] Siehe: https://www.inside-it.ch/de/post/die-post-sucht-digitalisierungs-know-how-20200706

A.12.8. Bürgerkonto (EADMIN)

Die Bürgerplattform / das Bürgerkonto von EADMIN[149] (Zusammenschluss der Firmen «Prime Technologies» und «Quicksite») bietet natürlichen Personen die Möglichkeit, sämtliche Gemeindedienstleistungen in einem zentralen Portal zu beziehen (sofern die Gemeinde dieses Portal einsetzt).

A.12.9. Elektronisches Patientendossier Schweiz

«Das elektronische Patientendossier (EPD) ist eine Sammlung persönlicher Dokumente mit Informationen rund um Ihre Gesundheit. Über eine sichere Internetverbindung sind diese Informationen sowohl für Sie als auch Ihre Gesundheitsfachpersonen jederzeit abrufbar. Sie selbst bestimmen, wer welche Dokumente wann einsehen darf.» [150] Beim elektronischen Patientendossier können die natürlichen Personen einerseits die eigenen Daten einsehen und andererseits Freigaben an Dritte für die Datenansicht vergeben.

A.12.10. DaziT

Mit dem Programm «DaziT» wird die digitale Transformation in der eidgenössischen Zollverwaltung (EZV) vorangetrieben[151]. Es werden bestehende Prozesse vereinfacht und digitalisiert sowie die Organisation weiterentwickelt. In diesem Zusammenhang entstehen auch neue Anwendungen[152], welche für UZ13 relevant sind. Ein Beispiel hierfür ist die App «QuickZoll» für natürliche Personen.

A.12.11. Programm EO-Digitalisierung

Die Abwicklung der Aktivitäten der Erwerbsersatzordnung (EO) soll ab 2025 elektronisch erfolgen153. In Rahmen der Abwicklung werden Personendaten zwischen den verschiedenen zuständigen Stellen und Unternehmen ausgetauscht.

A.12.12. Netzwerk Digitale Selbstbestimmung Schweiz

Das «Netzwerk Digitale Selbstbestimmung» verfolgt das Ziel, dass natürliche Personen selbstbestimmt über die Verwendung ihrer Daten verfügen können[154]. Die Initiative wird vom BAKOM (Bundesamt für Kommunikation) geführt.

A.12.13. HPi - Harmonisierung der Schweizer Polizeiinformatik

Mit dem HPi Programm soll die Polizei-Informatik der Schweiz harmonisiert werden[155]. Durch die Harmonisierung sollen die Effizienz und dadurch die Sicherheit der Bevölkerung verbessert und

---

[149] Siehe: https://www.eadmin.ch/de/N6492/burgerkonto.html

[150] Siehe: https://www.patientendossier.ch/de/bevoelkerung/kurz-erklaert

[151] Siehe: https://www.ezv.admin.ch/ezv/de/home/themen/dazit.html

[152] Siehe: https://www.ezv.admin.ch/ezv/de/home/themen/dazit/vereinfachung-und-digitalisierung/eingefuehrte-anwendungen.html

[153] Siehe: https://www.digitaldialog.swiss/en/digitalisierung-der-erwerbsersatzordnung-(eo)

[154] Ein aktuelles Arbeitspapier ist hier verfügbar: https://www.satw.ch/fileadmin/user_upload/documents/02_Themen/04_Digitalisierung/SATW-Digitale_Selbstbestimmung_Diskussionspapier.pdf

[155] Siehe: https://www.hpi-programm.ch/

gleichzeitig die Kosten gesenkt werden. Es werden folgende drei typischen Operationsmodelle gefördert[156]:

- Replikation: Es werden Lösungen einmal entwickelt und von den lokalen Organisationen unverändert in eigener Verantwortung in ihr Umfeld implementiert.
- Kooperation: Es werden gegenseitig Informationen/Daten zur Verfügung gestellt bzw. ausgetauscht – die Hoheit über die Daten bleibt jedoch bei der lokalen Organisation.
- Integration: Es wird für alle Partner eine gemeinsame Lösung aufgebaut und den Partnern wird der Zugriff auf die Lösung bzw. die entsprechenden Daten gewährt.

A.12.14. E-ID

Nach dem «Nein» zum E-ID-Gesetz vom 7 März 2021 besitzt die Schweiz weiterhin keine gesetzlich geregelte, national anerkannte elektrische Identität für natürliche Personen, welche von der öffentlichen Verwaltung anerkannt wird. Gemäss ersten Reaktionen aus dem Parlament soll möglichst bald ein neuer Gesetzesentwurf verfasst werden.

A.12.15. Kantonale elektronische Identitäten

Diverse Kantone haben eigene elektronische Identitäten aufgebaut. Beispiele sind hier das «BE-Login»[157], die «Schaffhauser eID+»[158], das Basler «eKonto»[159], die «frID» aus Fribourg[160], das «ZugLogin»[161] oder der «GuichetUnique» aus Neuenburg[162].

A.12.16. Städtische elektronische Identitäten

Auch erste Städte in der Schweiz setzen bereits auf eigene elektronische Identitäten – so beispielsweise die Stadt Zürich[163].

A.12.17. SwissID

Die SwissID[164] ist eine digitale Identität, welche von der «SwissSign Group AG» herausgegeben wird. Neben der Identitätsprüfung bietet die SwissID auch die Möglichkeit, den verschiedenen Akteuren spezifische Daten zur eigenen Identität freizugeben. Neben privaten Unternehmen (bspw. AXA Versicherungen, die Mobiliar) und halbstaatlichen Unternehmen (bspw. Post, SBB) setzen auch diverse Kantone (bspw. Aargau, St. Gallen, Graubünden) zumindest für gewisse Dienstleistungen die SwissID ein. Stand Sommer 2020 gab es bereits 1.4 Millionen registrierte Nutzer[165]. Einige Kantone verknüpfen Ihre elektronischen Identitäten mit der SwissID.

---

156 Siehe: https://www.hpi-programm.ch/HPi-PROGRAMM/Ziele

157 Siehe: https://www.belogin.directories.be.ch/cms/de/welcome.html

158 Siehe: https://sh.ch/CMS/Webseite/Kanton-Schaffhausen/Beh-rde/Services/Schaffhauser-eID--2077281-DE.html

159 Siehe: https://konto.egov.bs.ch/auth/login

160 Siehe: https://www.fr.ch/de/alltag/vorgehen-und-dokumente/e-governement

161 Siehe: https://www.zuglogin.ch/web/secure/

162 Siehe: https://www.guichetunique.ch/public/

163 Siehe: https://www.stadt-zuerich.ch/appl/lover/

164 Siehe: https://www.swissid.ch/

165 Siehe: https://www.itmagazine.ch/artikel/72642/SwissID_waechst_rasant_und_sorgt_fuer_Kritik.html

A.13. Zusätzliche Fragestellungen, welche für die E-Gov-Studie 2021 im Rahmen des Projektes UZ13 erarbeitet wurden

Es wurde die Möglichkeit genutzt, in der nationalen E-Gov-Studie 2021 einige Fragen im Zusammenhang mit UZ13 sowohl natürlichen Personen als auch der Verwaltung zu stellen. Die Fragen wurden im Projektteam initial entworfen und durch die externen Dienstleister, welche die Befragung durchführen, verfeinert. Besten Dank an Irem Kaynarca für die Unterstützung und die Koordination! Die Auswertung der E-Gov-Studie wird erst nach Abschluss der Machbarkeitsstudie im ersten Halbjahr 2022 publiziert werden.

A.13.1. Fragen an natürliche Personen

Folgende Fragen wurden an natürliche Personen gestellt:

- Haben Sie bereits einmal bei der öffentlichen Verwaltung oder einem Unternehmen von Ihrem gesetzlichen Recht zur Dateneinsicht Gebrauch gemacht?
  [single choice – ja / nein / weiss nicht]
- Wo haben Sie von Ihrem Recht zur Dateneinsicht Gebrauch gemacht?
  [single choice – Verwaltung / Unternehmen / beiden / weiss nicht]
- Aus welchem Grund haben Sie bis jetzt noch nie von Ihrem Recht zur Dateneinsicht Gebrauch gemacht?
  [multiple choice – mehrere Gründe]
- Inwiefern stimmen Sie folgenden Aussagen zu? Wenn ich meine Steuererklärung einreiche, dann … [Skala von 1-10]
  - bin ich ausreichend darüber informiert, was mit meinen Steuerdaten passiert.
  - gehe ich davon aus, dass die Behörden meine Steuerdaten erfolgreich vor unberechtigten Zugriffen schützen
  - gehe ich davon aus, dass die Behörden meine Steuerdaten nicht an unberechtigte Dritte weitergeben.
  - gehe ich davon aus, dass die Behörden meine Steuerdaten nur für gesetzlich definierte Anwendungsfälle verwenden.
  - gehe ich davon aus, dass die Behörden meine Steuerdaten automatisch an sämtliche berechtigten Behörden weiterleiten.
  - interessiert mich die Verwendung meiner Steuerdaten nicht weiter, denn ich vertraue den Behörden.
  - interessiert mich die Verwendung meiner Steuerdaten nicht weiter, denn diese ist ja gesetzlich geregelt.

Zudem wurden neben der Quantitativen Befragung auch Interviews durchgeführt, um mehr über die Gründe zu erfahren, warum natürliche Personen Daten eingesehen haben oder eben nicht.

A.13.2. Fragen an die öffentliche Verwaltung

Folgende Fragen wurden an Organisationseinheiten der öffentlichen Verwaltung gestellt:

- Wie oft erhalten Sie Anfragen von natürlichen Personen, welche Einsicht in ihre persönlichen Daten gemäss Datenschutzgesetz beantragen?
  [single choice - verschiedene Antwortmöglichkeiten bezüglich Häufigkeit]

- Wie viel Aufwand generiert eine solche Anfrage zur Einsicht in ihre persönlichen Daten gemäss Datenschutzgesetz?
  [single choice - verschiedene Antwortmöglichkeiten bezüglich Aufwand]

- Wie werden solche Anfragen zur Einsicht in ihre persönlichen Daten gemäss Datenschutzgesetz in der Regel an Sie herangetragen?
  [single choice - verschiedene Antwortmöglichkeiten zum für den Erstkontakt verwendeten Kommunikationskanal]

- Welche der folgenden Informationen werden von Ihrem wichtigsten IT-System zur Verarbeitung von Personendaten erfasst und gespeichert?
  [multiple choice – verschiedene Antwortmöglichkeiten zu Personendaten und allfälligen Log- und Metadaten]

A.14. Verbesserte Kommunikation als Sofort-Massnahme

Die typische Rechtsgrundlage (Gesetz und/oder Verordnung) für ein System zur Verarbeitung von Personendaten durch die öffentliche Verwaltung ist schnell einmal einige zehn oder sogar hunderte Seiten lang. Die Kommunikation der Verwendung von Personendaten kann beispielsweise über Info-Grafiken mit wenig Aufwand signifikant verbessert werden, wie folgendes Beispiel in Abbildung 27 zeigt[166]:

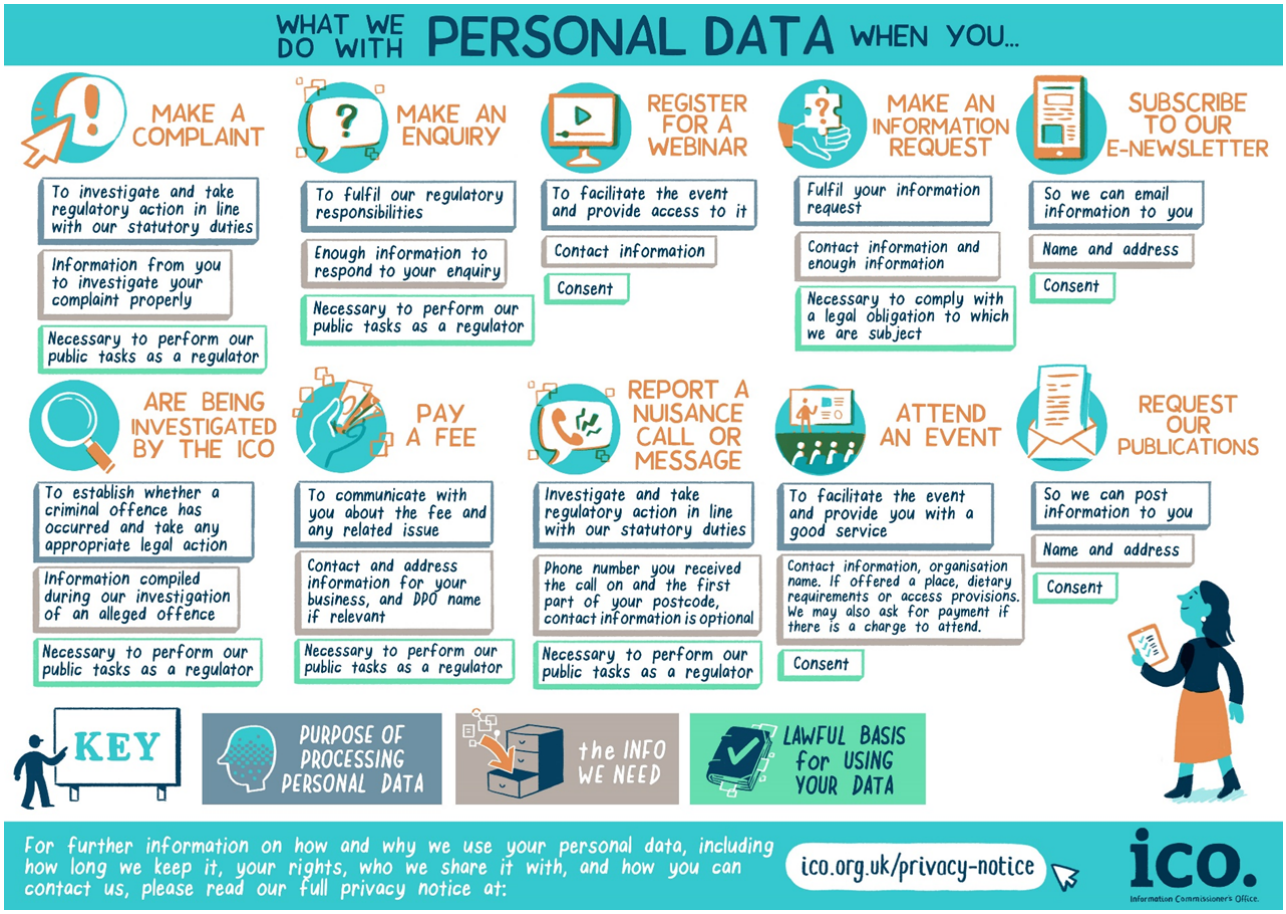

Abbildung 27: Infografik zur Verwendung von Personendaten basierend auf den Use-Cases (ico.org.uk - licensed under the Open Government Licence v3.0.)

Solche Infografiken können ansprechend präsentiert die wichtigsten Informationen zur Verwendung von Personendaten in einem Quellsystem abbilden, ohne die natürliche Person mit der gesamten rechtlichen Komplexität zu belasten. Da die verbesserte Kommunikation der Verwendung von Personendaten beispielsweise durch solche Infografiken mit wenig Aufwand umsetzbar ist, eignet sich diese als Sofort-Massnahme.

Alternative Formate wie Erklär-Videos bieten eine weitere Möglichkeit, um insbesondere auch die jüngere «Tik-Tok & Youtube»-Generation anzusprechen. Diese sind in der Umsetzung allerdings aufwändiger.

[166] Weitere schöne Beispiele findet man beispielsweise auf: www.dataqualitycampaign.org

A.15. Fragestellungen, welche mittels clickable Mockup oder Proof of Concept geklärt werden sollten

Folgende Fragen könnten mit einer geeigneten Umsetzung eines «clickable Mockups» oder eines «Proof of Concepts» einer Nachvollziehbarkeitslösung am Beispiel von einem oder wenigen ausgewählten Quellsystemen beantwortet werden:

- **Vertiefte Erkenntnisse zum Bedarf der natürlichen Personen nach einer Nachvollziehbarkeitslösung gewinnen:** Antworten auf beispielsweise folgende Fragestellungen sollen gesucht werden: Werden die relevanten Informationen angezeigt? Werden die Informationen gefunden? Werden die Informationen verstanden? Wird die Lösung regelmässig und von einer Vielzahl von natürlichen Personen benützt (nur Proof of Concept)?
- **Fördert die Nachvollziehbarkeitslösung Transparenz und Vertrauen:** Ist die gewählte Umsetzung und das Konzept einer Nachvollziehbarkeitslösung dazu geeignet, Transparenz und Vertrauen der natürlichen Personen gegenüber der Verwaltung zu erzeugen?
- **Umsetzung der Anforderungen auf Seite der Quellsysteme:** Welche Anpassungen sind auf der Seite der Quellsysteme notwendig, um die Anforderungen zur Anbindung an eine Nachvollziehbarkeitslösung umzusetzen?
- **Sammlung von Erfahrungen der User-Experience:** Wie müssen die vom Quellsystem gesammelten Log-Files aufbereitet und präsentiert werden, damit diese für die natürlichen Personen verständlich sind? Wird geeignete Funktionalität angeboten?
- **Überprüfung der Rahmenbedingungen:** Welche rechtlichen Anpassungen sind notwendig?

Mittels eines Proof of Concepts mit mehreren Quellsystemen könnten zudem folgende Fragen beantwortet werden:

- **Definition von Architektur und Prüfung Skalierbarkeit:** Ist die gewählte Architektur umsetzbar und skalierbar?
- **Definition und Testen von Schnittstellen:** Erfüllen die gewählten Schnittstellen die Anforderungen? Können diese mittels verschiedener Technologien effizient umgesetzt werden?
- **Aggregation und Darstellung von Daten aus mehreren Quellsystemen:** Wie können die Nachvollziehbarkeitsdaten aus verschiedenen Quellsystemen für die natürlichen Personen sinnvoll dargestellt und ggf. aggregiert werden?