Verhaltens-
KODEX

für den Betrieb von vertrauenswürdigen Datenräumen
basierend auf der digitalen Selbstbestimmung

vom Bundesrat gutgeheissen am 8. Dezember 2023

1. Einleitung

Am 30. März 2022 hat der Bundesrat den Bericht «Schaffung von vertrauenswürdigen Datenräumen basierend auf der digitalen Selbstbestimmung»[1] zur Kenntnis genommen. Dieser Bericht unterstreicht die Bedeutung von Daten und das Potenzial ihres Verwendungszwecks für die Schweiz und empfiehlt, die Schaffung und den Betrieb von vertrauenswürdigen und interoperablen Datenräumen aktiv zu fördern.

Datenräume sind organisatorische und technische Strukturen, welche Datennutzende und Datenanbietende miteinander verbinden und dadurch die Mehrfachnutzung von Daten ermöglichen. Datenräume stellen eine direkte Verbindung zwischen unterschiedlichen Akteuren auf der Angebots- und der Nachfrageseite von Daten her. Ein Datenraum ist in der Regel thematisch zentriert (bspw. Gesundheit, Mobilität, Finanzen etc.), umfasst prinzipiell Daten in einem weiten Sinn, d.h. verschiedene Datentypen (insb. Personendaten natürlicher Personen sowie Daten juristischer Personen und weitere Sachdaten[2], dynamische und/oder statische Daten etc.) und unterliegt einem Gouvernanzrahmen, welcher die Bedingungen für den Zugang zu Daten und deren Nutzung festlegt.

Für die Rolle der Stellen, die - in Abhängigkeit der rechtlichen, organisatorischen und praktischen Gegebenheiten des jeweiligen Datenraums - dessen Aufbau, Organisation und Gouvernanz festlegen, ist vorliegend die Rede von der sogenannten Datenraumträgerschaft. Diese Rolle kann auf verschiedene Akteure verteilt sein. Die weiteren für Datenräume relevanten Rollen sind im Anhang 1 genauer dargelegt. Der Verhaltenskodex dient für all diese Rollen als Orientierungsrahmen zur Ausgestaltung und Gouvernanz von vertrauenswürdigen Datenräumen.

Die Entwicklung von vertrauenswürdigen und interoperablen Datenräumen steht noch am Anfang, doch ihre Bedeutung wird in einer zunehmend digitalisierten Gesellschaft immer wichtiger. Sie bieten Potenzial für einen breiten Datenaustausch, schaffen Grundlagen für eine gemeinsame, vielseitigere und umfangreichere Nutzung von Daten sowie die Erschliessung von Synergien. Sie ermöglichen Innovation, eine effiziente und nachhaltige Nutzung bestehender Ressourcen sowie eine Befriedigung gesellschaftlicher und wirtschaftlicher Bedürfnisse. Um das Potenzial der vorhandenen Daten auszuschöpfen, bedarf es der Festlegung neuer Gouvernanzmechanismen und Standards, die darlegen, wie und unter welchen Bedingungen wir als Gesellschaft Daten künftig nutzen werden.

2. Ziel und Zweck des Verhaltenskodex

Der Aufbau von Datenräumen geschieht in einem Kontext von technologischer Komplexität, wachsenden Datenmengen in proprietären Silos und zunehmenden Fragen rund um die Kontrolle über Daten. Der Verhaltenskodex adressiert diese Herausforderungen, indem er die Ausgestaltung von vertrauenswürdigen Datenräumen konkretisiert. Indem Akteure in einem Datenraum Prozesse etablieren, welche die vertrauensstiftenden Verhaltensweisen umsetzen, können sie aktiv zum Vertrauen in eine verantwortungsvolle Nutzung von Daten in einem weiten Sinne beitragen. Im Sinne der digitalen Selbstbestimmung enthält der Verhaltenskodex Werkzeuge zur vertrauenswürdigen Ausgestaltung und Gouvernanz von Datenräumen sowie zum sicheren und kontrollierten Teilen und Nutzen von Daten für alle Beteiligten.

Der Verhaltenskodex definiert vier Grundprinzipien für die vertrauenswürdige Ausgestaltung von Datenräumen (siehe Abschnitt 7) und konkretisiert sie in Form von Empfehlungen mit entsprechenden möglichen Umsetzungsmassnahmen. Letztere sind entsprechend den Rollen gegliedert, die verschiedene Akteure innerhalb eines Datenraums einnehmen (siehe Anhang 1). Welche Empfehlungen für welche Akteure eines bestimmten Datenraums sinnvoll sind, ist im Rahmen des geltenden Rechts und anhand der Gegebenheiten des Datenraums und der legitimen Interessen aller Beteiligten zu prüfen. Nicht in jedem Fall ist die Umsetzung jeder Empfehlung sinnvoll, insbesondere, wenn im Fall von Zielkonflikten gewisse Empfehlungen zu priorisieren sind.

1. *Bericht Schaffung von vertrauenswürdigen Datenräumen basierend auf der digitalen Selbstbestimmung (BAKOM, EDA, März 2022).*
2. *Es ist zu beachten, dass aufgrund der Möglichkeit der Verknüpfung von Daten in Datenräumen eine trennscharfe Unterscheidung zwischen Personen- und Sachdaten künftig vermehrt erschwert wird. Die Unterscheidung von Personen- und Sachdaten fällt den verantwortlichen Akteuren innerhalb eines Datenraumes zu.*

3. Adressaten des Verhaltenskodex

Adressaten des Verhaltenskodex sind alle privaten und öffentlichen Akteure, die sich an einem Datenraum beteiligen. Diese Akteure nehmen eine oder mehrere dieser vier Rollen ein: Datenraumträgerschaft, Datenvermittelnde, Datenanbietende und Datennutzende (siehe Anhang 1). Entsprechend beziehen sich sowohl die nachstehenden Empfehlungen als auch deren möglichen Umsetzungsmassnahmen auf diese vier Rollen. Der Verhaltenskodex kann auch als Orientierung für allfällige zukünftige Datenraumakteure oder sonstige interessierte Kreise dienen.

4. Mehrwert des Verhaltenskodex

Mit dem Verhaltenskodex soll ein Grundverständnis hinsichtlich vertrauensstiftender Verhaltensweisen in Datenräumen gefördert werden, sodass letztere von Individuen, Unternehmen sowie öffentlichen Stellen als sicher erachtet und genutzt werden. Der Verhaltenskodex zeigt damit auf, wie ein selbstbestimmter und vertrauenswürdiger Umgang mit Daten gefördert und das Nutzungspotenzial von Daten besser ausgeschöpft werden kann.

Die Befolgung des Verhaltenskodex bringt aus gesellschaftlicher und wirtschaftlicher Perspektive folgende Mehrwerte:

1. Stärkeres Vertrauen in den Umgang mit Daten ermöglicht eine vielseitigere und umfangreichere Datennutzung, welche Raum für Innovationen, neuartige Geschäftsmodelle und optimierte sowie personalisierte Dienstleistungen bietet. Dies trägt auch dazu bei, dass gesamtgesellschaftliche Herausforderungen, wie beispielsweise der Klimawandel, vermehrt mit datenbasierten Methoden angegangen werden können.
2. Der Verhaltenskodex ermöglicht den anwendenden Akteuren eines vertrauenswürdigen Datenraums, eine Vorreiterrolle in neuen und digitalen Geschäftsmodellen einzunehmen.
3. Die Schaffung von Vertrauen und Akzeptanz in eine angebotene Dienstleistung und die verwendeten Technologien wirkt sich positiv auf das Erlebnis der betroffenen Adressaten und den wirtschaftlichen Erfolg aus.
4. Anwendende Akteure prägen die Anwendung und Weiterentwicklung des Verhaltenskodex mit.
5. Es entsteht eine praxisbezogene Gemeinschaft, welche Erfahrungen im Betrieb von vertrauenswürdigen Datenräumen austauschen kann.
6. Letztlich unterstützt der Verhaltenskodex ein abgestimmtes Zielbild von Bund, Privatsektor und Zivilgesellschaft betreffend vertrauenswürdiger Datenräume.

5. Rechtliche Einordnung des Verhaltenskodex

Je nach Kontext und involvierten Akteuren müssen Datenräume in ihren verschiedenen Funktionsweisen und Ausrichtungen unterschiedlichen Herausforderungen Rechnung tragen. Gewichtung sowie Umsetzung der verschiedenen Verhaltensempfehlungen und Umsetzungsmassnahmen müssen deshalb je nach Anwendungsbereich und Sensibilität der Daten ausgestaltet und priorisiert werden können. Entsprechend dient dieser freiwillige Verhaltenskodex durch die Statuierung rechtlich nicht verbindlicher Verhaltensempfehlungen als Hilfestellung für private und öffentliche Akteure, die im für sie jeweils geltenden Kontext und rechtlichen Rahmen an der Schaffung von Datenräumen arbeiten oder sich in solchen bewegen.

Es gilt jedoch zu beachten, dass gewisse Anforderungen des Verhaltenskodex Überschneidungen mit bestehenden gesetzlichen und spezialgesetzlichen Anforderungen haben (bspw. im Datenschutzgesetz). Der Verhaltenskodex setzt hier und in allen anderen Bereichen die vollständige und umfassende Einhaltung der bestehenden gesetzlichen Grundlagen voraus. Entsprechend ersetzt die Umsetzung dieses Verhaltenskodex auch keine umfassende Prüfung der Einhaltung relevanter Rechtsvorschriften oder allfälliger branchenspezifischer Normen.

Vertrauen setzt jedoch mehr als das Einhalten von Gesetzen voraus. Der Verhaltenskodex ist daher bewusst breiter angelegt als bestehende gesetzliche Grundlagen, wie bspw. im Bereich des Datenschutzes. Als Instrument der Selbstregulierung ergänzt der Verhaltenskodex den bestehenden Rechtsrahmen, indem er freiwillige und weitergehende Verhaltensweisen für die Erreichung des Zielbildes vertrauenswürdiger Datenräume basierend auf der digitalen Selbstbestimmung propagiert. Entsprechend ist der Verhaltenskodex rechtlich nicht verbindlich, verfolgt aber einen gewissen normativen Anspruch. Es wird davon ausgegangen, dass für

alle Beteiligten aufgrund ihres Interesses an vertrauenswürdigen Datenräumen ein hoher Anreiz besteht, sich insofern an den Verhaltenskodex zu halten, als sie sich seriös damit auseinandersetzen und die Umsetzung der für sie relevanten Verhaltensempfehlungen in ihrem Kontext genau prüfen.

6. Entwicklung des Verhaltenskodex

Die nachstehenden Empfehlungen und dazugehörigen Umsetzungsmassnahmen in Anhang 2 wurden in Form der koordinierten Selbstregulierung unter der Leitung des Bundes in einem inklusiven Prozess von verschiedenen Akteuren aus Privatwirtschaft, Akademie, Zivilgesellschaft und der öffentlichen Verwaltung ausgearbeitet. Es ist denkbar, dass der Verhaltenskodex durch eine neue Gesetzgebung ergänzt oder abgelöst wird, wie sie die Kommission für Wissenschaft, Bildung und Kultur des Ständerats in ihrer Motion 22.3890 vom 22. August 2022 vorschlägt, und dass dabei die inhaltlichen Gewichte verschoben werden.

7. Grundprinzipien

Die nachfolgenden Verhaltensempfehlungen zeigen auf, wie die Grundprinzipien innerhalb eines Datenraums umgesetzt werden können. Sie werden in Anhang 2 weiter konkretisiert und als mögliche Umsetzungsmassnahmen den Rollen des Datenraums (vgl. Abschnitt 3 und Anhang 1) zugeordnet.

Transparenz

Das Grundprinzip der Transparenz sieht einen einfachen und transparenten Zugang zu wichtigen Informationen vor.

1. **Dokumentation**: Notwendige Informationen sind so dokumentiert und zugänglich, dass sich alle involvierten Akteure im Datenraum ein klares Bild von der Datennutzung machen können (insb. Inhalte, Erhebung, Speicherung, Aufbewahrung, Verwendung, Veränderung, Bekanntgabe, Weitergabe, Archivierung, Löschung oder Vernichtung von Daten). Dasselbe gilt für die Nutzungszwecke der Daten.
2. **Organisation**: Es herrscht Transparenz über das Geschäftsmodell, die Form und die Organisation des Datenraums.
3. **Verständlichkeit**: Informationen und Daten in Zusammenhang mit dem Datenraum werden einfach zugänglich gemacht und sind sowohl verständlich als auch zielgruppengerecht dargestellt.
4. **Nachvollziehbarkeit**: Es wird sichergestellt, dass die Herkunft der bereitgestellten Daten nachvollziehbar sowie, insbesondere bei Personendaten, Umfang und Zweck der Datennutzung innerhalb des Datenraums vorhersehbar sind.
5. **Zugang**: Akteure eines Datenraums haben einfachen und hürdenfreien Zugang zu Daten und Metadaten. Das bedeutet, dass auf Daten und Metadaten zeitnah und maschinenlesbar zugegriffen werden kann.

Kontrolle

Das Grundprinzip Kontrolle gewährleistet, dass alle Akteure ihren Rollen entsprechend die Möglichkeit haben, ihre Daten sowie den Zugriff darauf zu verwalten.

6. **Kontrollinstrumente**: Innerhalb eines vertrauenswürdigen Datenraums verfügen alle Akteure ihren Rollen entsprechend über die notwendigen Kontrollinstrumente für eine sichere Datennutzung, insbesondere für Personendaten.
7. **Weitergabe**: Sollte ein Datenraum die Weitergabe von Daten über den Datenraum hinaus vorsehen, so ist die Kontrolle über eine solche Weitergabe gewährleistet. Dies ist insbesondere der Fall, wenn es sich um Personendaten handelt.
8. **Wahlfreiheit**: Wo keine gesetzlichen Pflichten bestehen, ist die Teilnahme an einem Datenraum freiwillig. Die Teilnahme selbst richtet sich nach datenraumspezifischen Bedingungen.
9. **Sicherheit**: In einem Datenraum bestehen klare Prozesse, um Sicherheitsrisiken für den Datenraum und die beteiligten Akteure zu identifizieren und ggf. zu mindern.

Fairness

Das Grundprinzip Fairness verlangt eine gerechte Behandlung aller Akteure in einem Datenraum.

10. **Verhältnismässigkeit**: Austausch, Nutzung und Mehrfachnutzung von Daten innerhalb eines Datenraums basieren auf dem Verhältnismässigkeitsprinzip.
11. **Diskriminierungsfreiheit**: Datenraumspezifische Bedingungen und Betrieb eines Datenraums sind diskriminierungsfrei ausgestaltet und die Möglichkeit zur Teilnahme als Akteur ist nach sachlich objektiven Kriterien zu gewährleisten.
12. **Interessenausgleich**: Es besteht ein Interessenausgleich zwischen den Akteuren in einem Datenraum.
13. **Datenqualität**: Alle Akteure innerhalb eines Datenraums streben eine hohe Datenqualität an. Daten haben direkte Auswirkungen auf die Gestaltung von Produkten und Dienstleistungen. Entsprechend können qualitativ unzulängliche Datensätze zu Diskriminierung und Ungleichbehandlungen führen.
14. **Besonderer Schutz von Kindern und Jugendlichen**: Kinder und Jugendliche geniessen aufgrund der geringen Erfahrung besonderen Schutz, wenn sie an einem Datenraum teilnehmen.

Effektivität

Das Grundprinzip der Effektivität trägt dazu bei, Nützlichkeit und Nachhaltigkeit von Datenräumen zu maximieren.

15. **Umsetzung**: Die in einem Datenraum geltenden Bedingungen werden effektiv angewendet und umgesetzt.
16. **Interoperabilität**: Alle Akteure fördern, wo immer möglich und relevant, die Interoperabilität von Datenräumen.
17. **Agilität**: Datenräume entwickeln sich kontinuierlich weiter und können sich veränderten Gegebenheiten schnell und flexibel anpassen.
18. **Nachhaltigkeit**: Alle Akteure setzen sich für die ökologische, soziale und wirtschaftliche Nachhaltigkeit des Datenraums ein.

8. Praxisaustausch

Um eine breite und wirksame Anwendung des Verhaltenskodex (vergleichbare Ergebnisse in vergleichbaren Situationen) sowie deren Weiterentwicklung zu fördern, wird angeregt, dass Datenraumträgerschaften regelmässig einen Praxisaustausch organisieren. Sie verfolgen dabei einen Multi-Stakeholderansatz und sind auf die Interdisziplinarität des Praxistaustauschs bedacht. Damit ein Praxisaustausch zustande kommt, werden entsprechende Aktivitäten durch die Datenraumträgerschaften definiert. Dadurch werden «best practices» gefördert, die Mitsprache verschiedener Akteure gewährleistet sowie Kapazitäten aufgebaut. Die Datenraumträgerschaften erstatten öffentlich Bericht über Inhalt und Form des Praxisaustauschs.

9. Umsetzung

Die unterzeichnenden Organisationen und Einheiten veröffentlichen in regelmässigem Abstand einen Bericht über ihre Umsetzung der Verhaltensempfehlungen und Massnahmen. Zu Zwecken der Vergleichbarkeit folgt der Bericht einer einheitlichen Struktur. Daneben ist es den Unterzeichnenden freigestellt, weitergehende Massnahmen zu ergreifen (bspw. gegenseitiges Peer Review, Etablierung von Data Assemblies etc.).

10. Verhältnis zu anderen Vorhaben des Bundes

Nebst dem Verhaltenskodex für den Betrieb von vertrauenswürdigen Datenräumen erarbeitete das Bundesamt für Statistik einen «Verhaltenskodex für menschenzentrierte und vertrauenswürdige Datenwissenschaft». Dieser enthält vertrauenswürdige Verhaltensweisen für datenwissenschaftliche Vorhaben des Bundes, mit denen datenbasierte Erkenntnisse gewonnen und für Problemstellungen genutzt werden können. Beide Kodizes fördern somit in ihren jeweiligen Anwendungsbereichen die Datennutzung unter vertrauenswürdigen Bedingungen und verfolgen somit gleiche Ziele.

Mit der Motion 22.3890 WBK-S v. 22.08.2022 Rahmengesetz für die Sekundärnutzung von Daten wurde der Bundesrat beauftragt, in einem Rahmengesetz Grundlagen zu schaffen, damit spezifische Infrastrukturen für die Sekundärnutzung von Daten in strategisch relevanten Bereichen rasch initialisiert und aufgebaut werden können. Der Verhaltenskodex kann hierzu wichtige Erkenntnisse liefern.

Anhang 1: Rollen in einem Datenraum

Datenräume sind organisatorische und technische Strukturen, welche Datennutzende und Datenanbietende miteinander verbinden und dadurch den Austausch und die Mehrfachnutzung von Daten ermöglichen. Datenräume stellen somit eine direkte Verbindung zwischen unterschiedlichen Akteuren auf der Angebots- und der Nachfrageseite von Daten her. Ein Datenraum ist in der Regel thematisch zentriert und weist einen Gouvernanzrahmen auf, welcher die datenraumspezifischen Bedingungen für den Zugang und die Nutzung von Daten innerhalb des Datenraums festlegt. Aufbau, Organisation und Gouvernanz eines Datenraums werden dabei, wo immer möglich, in einem inklusiven Prozess durch die Datenraumträgerschaft in Abstimmung mit den weiteren Akteuren eines Datenraums festgelegt. Innerhalb eines Datenraums können anhand der eingenommenen Funktionen und Verantwortung insgesamt vier Rollen identifiziert werden. Dabei kann ein Akteur unterschiedliche Rollen einnehmen und die Teilnahme ist nicht auf einen einzelnen Datenraum begrenzt. Zudem kann eine hier idealtypisch erfasste Rolle auf mehrere Akteure verteilt sein.[3] Für das Funktionieren eines Datenraums sind insbesondere die Rollen der Datenraumträgerschaft, der Datenvermittelnden, der Datenanbietenden und der Datennutzenden notwendig. Abbildung 1 zeigt eine vereinfachte Übersicht dieser Rollen:

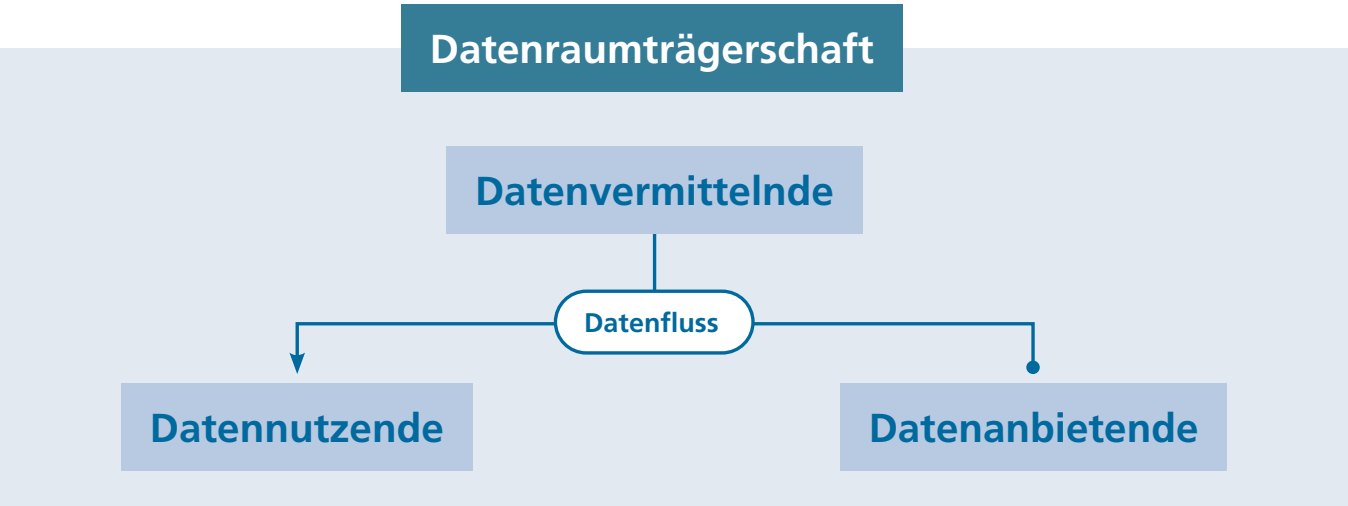

Abbildung 1: Übersicht Rollen im Datenraum

3. *Das ist insbesondere der Fall, wenn Staatsorgane Aufgaben der Trägerschaft übernehmen. Dies weil gemäss dem Verfassungsgrundsatz der Gewaltenteilung das Festlegen, Anwenden und Durchsetzen von Regeln grundsätzlich auf verschiedene Staatsorgane zu verteilen ist.*

A. Rolle und Verantwortung / Funktion

Rolle	Verantwortung / Funktion
Datenraumträgerschaft	In der Rolle der Datenraumträgerschaft werden alle Funktionen versammelt, die den datenraumspezifischen Gouvernanzrahmen betreffen, d.h. konkret die Etablierung, Gestaltung, Festigung und ggf. die Anwendung der Bedingungen und dazugehörigen Umsetzungssystemen innerhalb eines Datenraums im jeweiligen Fachkontext. In diesem Sinn stellt die Datenraumträgerschaft mittels dem Gouvernanzrahmen sicher, dass die Vertrauenswürdigkeit und die Interoperabilität des Datenraums gegeben sind und trägt somit massgeblich zu einer Vertrauenskultur bei.
Datenvermittelnde	Datenvermittelnde bieten Dienste für eine gemeinsame Datennutzung an. Sie stellen den Austausch von Daten zwischen Angebot und Nachfrage sicher. Datenvermittelnde können sowohl Organisationen als Betreiber von Infrastruktur für den Austausch von Daten (wie bspw. Software, physische Infrastruktur) sein, aber auch Anbieter von subsidiären Dienstleistungen wie Identifikation oder Authentifikation. Die Dienste können für einen spezifischen Datenraum oder als generelle Dienstleistung für unterschiedliche Anwendungen angeboten werden.
Datennutzende	Datennutzende nutzen Daten und/oder datenbezogene Services des Datenraums. Sie können je nach Ausgestaltung des Datenraums sowohl Organisationen als auch natürliche Personen sein.
Datenanbietende	Datenanbietende haben die Entscheidungshoheit zur Gewährung oder Widerrufung von Zugriffs- und Nutzungsrechten auf bestimmte Daten. Sie können Daten innerhalb eines Datenraums bereitstellen. Je nach Datenraum können Datenanbietende sowohl Organisationen als auch natürliche Personen sein. Gemäss Datenschutzrecht sind betroffene Personen natürliche Personen, über die Personendaten bearbeitet werden.[4] Innerhalb eines Datenraums können betroffene Personen selbst als Datenanbietende auftreten. Das ist der Fall, wenn sie selber ihre Daten in den Datenraum geben. In der Rolle der Datenanbietenden können jedoch auch Dritte auftreten, insbesondere Unternehmen, die Daten juristischer Personen und weitere Sachdaten sowie Daten über ihre Kunden oder weitere Personen anbieten. Der Verhaltenskodex statuiert lediglich Verhaltensempfehlungen für jene Konstellationen des Datenanbietens/Datenaustauschs, die innerhalb eines Datenraums stattfinden. In jedem Fall, d.h. auch dann, wenn betroffene Personen in keinem direkten Verhältnis mit dem Datenraum stehen, gilt der bestehende Rechtsrahmen, insbesondere das Datenschutzrecht. Dies bedeutet auch, dass innerhalb von einzelnen Datenräumen in jedem Fall die vom Datenschutzgesetz verlangten Rollen (bspw. Verantwortlicher, Auftragsbearbeiter etc.) benannt werden müssen.

4. *Vgl. Art. 5 lit. b DSG.*

B. Rollen und Akteure

Die Rolle der Datenraumträgerschaft kann unter Umständen durch ein Gremium mit Vertretenden von mehreren Organisationen oder einer Organisation besetzt werden. Mindestens im staatlichen Kontext wird sie aber in mehrere Teilrollen mehrerer Organe auseinanderfallen (Vgl. Anhang 1.A).

Aufgrund der Funktionen von Datenvermittelnden handelt es sich in aller Regel um juristische Personen des privaten und/oder des öffentlichen Rechts sowie um öffentliche Organe, die mit öffentlichen Aufgaben betraut sind.

Die Rolle des Datennutzenden und Datenanbietenden kann von natürlichen und juristischen Personen des privaten und/oder öffentlichen Rechts sowie von öffentlichen Organen, die mit öffentlichen Aufgaben betraut sind, wahrgenommen werden.

Sofern juristische Personen des öffentlichen Rechts sowie öffentliche Organe (insb. alle Organe des Bundes und der Kantone, die mit öffentlichen Aufgaben des Bundes oder der Kantone betraut sind) eine der vier Rollen des Datenraums übernehmen, gilt das Legalitätsprinzip gemäss Art. 5 Abs. 1 BV, bzw. bedarf es einer gesetzlichen Grundlage. Der Verhaltenskodex kann folglich als Orientierungshilfe für die Ausgestaltung dieser gesetzlichen Grundlagen staatlichen Handelns dienen. Ähnliches gilt im Kontext privater Akteure, in welchem der Verhaltenskodex als Orientierungshilfe für die Ausgestaltung vertraglicher Grundlagen oder organisationsinterner Regelungen dienen kann.

Anhang 2: Mögliche Umsetzungsmassnahmen

Dieser Anhang konkretisiert die Empfehlungen mit entsprechenden möglichen Umsetzungsmassnahmen. Die Umsetzungsmassnahmen sind entsprechend den Rollen gegliedert, die Akteure innerhalb eines Datenraums einnehmen können. Welche Empfehlungen und Umsetzungsmassnahmen für welche Akteure eines bestimmten Datenraums sinnvoll sind, ist anhand der Gegebenheiten des Datenraums, der legitimen Interessen aller Beteiligten und im Rahmen des geltenden Rechts zu prüfen. Nicht in jedem Fall ist die Umsetzung jeder Empfehlung und Massnahme sinnvoll. Eine möglichst konsequente Umsetzung der Empfehlungen und Massnahmen ist mit Blick auf die Vertrauenswürdigkeit von Datenräumen jedoch zielführend.

Um die praktische Anwendung der Umsetzungsmassnahmen zu unterstützen, verweist der Anhang an verschiedenen Stellen auf bereits existierende rechtliche Pflichten, die in einem engeren oder weiteren Zusammenhang mit der jeweiligen Massnahme stehen. Der Verhaltenskodex setzt hier und in allen anderen Bereichen die vollständige und umfassende Einhaltung der bestehenden gesetzlichen Grundlagen voraus. Die Verweise erheben keinen Anspruch auf Vollständigkeit. Der Begriff «Daten» wird im gesamten Verhaltenskodex in einem weiten Sinne verstanden (das beinhaltet bspw. Personendaten natürlicher Personen sowie Daten juristischer Personen, Sachdaten, dynamische und/oder statische Daten etc.). Wo explizit ein bestimmter Datentyp gemeint ist (bspw. Personendaten) ist dies entsprechend vermerkt oder referenziert.

TRANSPARENZ

Empfehlung 1: Dokumentation

Notwendige Informationen sind so dokumentiert und zugänglich, dass sich alle involvierten Akteure im Datenraum ein klares Bild von der Datennutzung machen können (insb. Inhalte, Erhebung, Spteicherung, Aufbewahrung, Verwendung, Veränderung, Bekanntgabe, Weitergabe, Archivierung, Löschung oder Vernichtung von Daten). Dasselbe gilt für die Nutzungszwecke der Daten.

Mögliche Umsetzungsmassnahmen zu Empfehlung 1

Datenraumträgerschaften	Datenvermittelnde	Datennutzende	Datenanbietende
1.1.1 Datenraumträgerschaften stellen die relevanten Informationen über den im Datenraum geltenden generellen Prozess der Datennutzung auf transparente Weise den anderen Akteuren des Datenraums zur Verfügung.	1.2.1 Datenvermittelnde unterstützen Datenraumträgerschaften, indem sie relevante Informationen über den im Datenraum geltenden generellen Prozess der Datennutzung zur Verfügung stellen.	1.3.1 Datennutzende stellen Informationen über die genaue Art und Weise der Datennutzung für Datenraumträgerschaften, Datenvermittelnde und Datenanbietende bereit. Bei Mehrfachnutzung der Daten übernehmen die jeweiligen Datennutzenden die Aufgabe, die anderen Akteure über die neuen möglichen Nutzungszwecke zu informieren.[6] In einem Open-Government-Data-Kontext ist diese Umsetzungsmassnahme nicht zweckmässig.	1.4.1 Datenanbietende machen transparent, aus welchen Quellen die angebotenen Daten kommen und für was sie verwendet werden dürfen.[5]
1.1.2 Datenraumträgerschaften gewährleisten die transparente Bereitstellung von Informationen und Kontrollen bezüglich der Zugriffsrechte durch Externe. Ausserdem sind Informationen darüber zugänglich, wie diese Zugriffsrechte kontrolliert und sichergestellt werden.	1.2.2 Datenvermittelnde überwachen den Zugang zu Daten von Externen. Wo relevant, stellen sie sicher, dass die Genehmigung für die Übertragung an Externe besteht.[7]		1.4.2 Datenanbietende machen gegenüber betroffenen Akteuren des Datenraums transparent, wann und unter welchen Bedingungen sie Daten an Externe weitergeben. Im Falle von Personendaten machen sie auch transparent, wem sie welche Daten bereitgestellt haben.[8]
	1.2.3 Datenvermittelnde stellen Informationen über die technischen und organisatorischen Massnahmen bereit, die sie treffen, um die Identifizierung und Autorisierung der beteiligten Akteure innerhalb eines Datenraums sicherzustellen.[9]		

5. *Betreffend Personendaten i.S.v. Art. 5 lit. a DSG vgl. insb. Art. 25-27 DSG zum Auskunftsrecht.*
6. *Betreffend Personendaten i.S.v. Art. 5 lit a DSG vgl. insb. Art. 12, 19-20 DSG.*
7. *Betreffend Personendaten i.S.v. Art. 5 lit. a DSG vgl. insb. Art. 9 Abs. 3 DSG.*
8. *Betreffend Personendaten i.S.v. Art. 5 lit. a DSG vgl. insb. Art. 19 DSG.*
9. *Betreffend Personendaten i.S.v. Art. 5 lit. a DSG vgl. insb. Art. 8 und Art. 9 Abs. 2 DSG*

1.1.4 Datenraumträgerschaften sorgen für transparente Informationen über die im Datenraum vorgesehenen Bedingungen für allfällige Datenübertragungen ins Ausland.	1.2.4 Datenvermittelnde sorgen bei Datenübertragungen ins Ausland für ein angemessenes Datenschutzniveau, insbesondere bei sensiblen Daten (d.h. besonders schützenswerten Personendaten oder wertvollen Sachdaten). In Bezug auf Personendaten informieren sie über die unternommenen Anstrengungen, einen für die in der Schweiz geltenden Bedingungen angemessenen Schutz zu gewährleisten.[10]		1.4.4 Datenanbietende sorgen bei Datenübertragungen ins Ausland für ein angemessenes Datenschutzniveau, insbesondere bei sensiblen Daten (d.h. besonders schützenswerten Personendaten oder wertvollen Sachdaten). In Bezug auf Personendaten informieren sie über die unternommenen Anstrengungen, einen für die in der Schweiz geltenden Bedingungen angemessenen Schutz zu gewährleisten.[11]

10. Betreffend Personendaten i.S.v. Art. 5 lit. a DSG vgl. insb. Art. 16-18 DSG.
11. Ibid.

Empfehlung 2: Organisation
Es herrscht Transparenz über das Geschäftsmodell, die Form und die Organisation des Datenraums.

Mögliche Umsetzungsmassnahmen zu Empfehlung 2

Datenraumträgerschaften	Datenvermittelnde	Datennutzende	Datenanbietende
2.1.1 Datenraumträgerschaften stellen Informationen über die im Datenraum geltenden Bedingungen sowie über die beteiligten Akteure, ihre Rollen und Positionen im Entscheidungsprozess transparent zur Verfügung.	2.2.1 Datenvermittelnde stellen Informationen über die Infrastruktur und die technischen Dienste des Datenraums zur Verfügung.		
2.1.2 Datenraumträgerschaften gewährleisten transparente Informationen über den Aufbau und die rechtliche und finanzielle Funktionsweise des Datenraums.			
2.1.3 Datenraumträgerschaften klären und regeln die Rechte und Pflichten der verschiedenen Akteure so verbindlich wie möglich (z.B. durch Checklisten oder Musterverträge oder durch Gesetz und Verordnung). Feedback-Mechanismen werden eingerichtet, um die Rollen anzupassen und zu verbessern.			
2.1.4 Datenraumträgerschaften ergreifen Sicherheitsmassnahmen, um die Durchführung zentraler Aufgaben und die notwendigen Entscheidungsprozesse zu gewährleisten sowie das Risiko von Cyberangriffen zu minimieren.			

Empfehlung 3: Verständlichkeit
Informationen und Daten in Zusammenhang mit dem Datenraum werden einfach zugänglich gemacht und sind sowohl verständlich als auch zielgruppengerecht dargestellt.

Mögliche Umsetzungsmassnahmen zu Empfehlung 3			
Datenraumträgerschaften	**Datenvermittelnde**	**Datennutzende**	**Datenanbietende**
3.1.1 Datenraumträgerschaften stellen sicher, dass die Informationen und Daten angemessen, lesbar und korrekt sind. Die Sprache und die Kommunikationsmethoden sind den Adressaten angepasst, um das Verständnis zu fördern.	3.2.1 Alle Informationen über die Funktion und Struktur des Datenraums müssen wo sinnvoll maschinenlesbar zugänglich sein, um eine einfache Verwendung zu ermöglichen.		
	3.2.2 Datenvermittelnde sorgen für ein leichtes Verständnis der Informationen, z.B. durch visuelle oder audiovisuelle Hilfsmittel wie Datenschutzsymbole, erklärende Videos oder Podcasts, die komplexe Themen auf allgemeinverständliche Weise darstellen.		
	3.2.3 Sensible Daten (d.h. besonders schützenswerte Personendaten oder wertvolle Sachdaten) werden bei ihrer Erhebung und der Einholung der Einwilligung zur weiteren Nutzung mit einer besonderen Kennzeichnung versehen.		
3.1.4 Datenraumträgerschaften stellen für individuelle Fragen eine Kontaktstelle zur Verfügung.			

Empfehlung 4: Nachvollziehbarkeit
Es wird sichergestellt, dass die Herkunft der bereitgestellten Daten nachvollziehbar sowie, insbesondere bei Personendaten, Umfang und Zweck der Datennutzung innerhalb des Datenraums vorhersehbar sind.

Mögliche Umsetzungsmassnahmen zu Empfehlung 4			
Datenraumträgerschaften	**Datenvermittelnde**	**Datennutzende**	**Datenanbietende**
	4.2.1 Datenvermittelnde stellen Zugriffsprotokolle zur Verfügung, damit Datenanbietende nachvollziehen können, wer wann auf welche ihrer Daten zugegriffen hat.[12]		4.4.1 Datenanbietende kennzeichnen die Quelle der Daten, sodass die Datenherkunft vollständig nachvollzogen werden kann (Lineage).
4.1.2 Datenraumträgerschaften informieren die Datenanbietenden über die potenziellen generellen Risiken der Datenbereitstellung.	4.2.2 Datenvermittelnde informieren die Datenanbietenden über die potenziellen generellen Risiken der Datenbereitstellung.	4.3.2 Datennutzende informieren die Datenanbietenden über die potenziellen konkreten Risiken der Datenbereitstellung.[13]	4.4.2 Datenanbietende werden über die möglichen Risiken der Bereitstellung ihrer Daten informiert.[14]
	4.2.3 Datenvermittelnde erstellen Fehlerprotokolle und informieren alle betroffenen Akteure über diese.		

12. *Betreffend Personendaten i.S.v. Art. 5 lit. a DSG vgl. insb. Art. 12 DSG und Art. 4 DSV.*
13. *Betreffend Personendaten i.S.v. Art. 5 lit. a DSG vgl. insb. Art. 22-24 DSG.*
14. *Betreffend Personendaten i.S.v. Art. 5 lit. a DSG vgl. insb. Art. 24 Abs. 3 und Art. 25-26 DSG.*

Empfehlung 5: Zugang
Akteure eines Datenraums haben einfachen und hürdenfreien Zugang zu Daten und Metadaten. Das bedeutet, dass auf Daten und Metadaten zeitnah und maschinenlesbar zugegriffen werden kann.

Mögliche Umsetzungsmassnahmen zu Empfehlung 5

Datenraumträgerschaften	Datenvermittelnde	Datennutzende	Datenanbietende
5.1.1 Datenraumträgerschaften stellen sicher, dass ein standardisierter Metadatenkatalog und Datenmodelle, die das schnelle Auffinden von Daten ermöglichen, zur Verfügung gestellt werden.	5.2.1 Datenvermittelnde erstellen einen standardisierten Metadatenkatalog und Datenmodelle.	5.3.1 Datennutzenden wird ein Metadatenkatalog zur Verfügung gestellt.	5.4.1 Datenanbietende erfassen ihre Metadaten entsprechend dem zur Verfügung gestellten Metadatenkatalog.
5.1.2 Datenraumträgerschaften stellen sicher, dass die Mechanismen zur Wahrnehmung des Zugangsrechts harmonisiert und für Datenanbietende leicht zugänglich sind.	5.2.2 Datenvermittelnde harmonisieren die Mechanismen zur Wahrnehmung des Zugangsrechts und ermöglichen den Datenanbietenden einen einfachen Zugang zu den Mechanismen.	5.3.2 Die Mechanismen zur Ausübung des Zugangsrechts sind harmonisiert und für Datennutzende leicht zugänglich.	5.4.2 Die Mechanismen zur Ausübung des Zugangsrechts sind harmonisiert und für Datenanbietende leicht zugänglich.

KONTROLLE

Empfehlung 6: Kontrollinstrumente

Innerhalb eines vertrauenswürdigen Datenraums verfügen alle Akteure über die notwendigen Kontrollinstrumente für eine sichere Datennutzung, insbesondere für Personendaten.

Mögliche Umsetzungsmassnahmen zu Empfehlung 6

Datenraumträgerschaften	Datenvermittelnde	Datennutzende	Datenanbietende
6.1.1 Datenraumträgerschaften stellen sicher, dass alle Datennutzenden, Datenvermittelnden und Datenanbietenden innerhalb eines Datenraums über die notwendigen Kontrollinstrumente für die Datennutzung verfügen.	6.2.1 Datenvermittelnde informieren über die bestehenden Kontrollinstrumente für die Datennutzung. Sie holen zudem wo immer nötig die informierte Einwilligung zur Bearbeitung der Daten ein.[15] Darüber hinaus sorgen Datenvermittelnde für eine zeitliche und inhaltliche Beschränkung der Datennutzung, d.h. die Einwilligung kann nicht in Form einer Blankovollmacht erteilt werden.		6.4.1 Wo keine gesetzlichen Pflichten bestehen, haben Datenanbietende die Möglichkeit, der Verwendung ihrer Daten für einen bestimmten Zweck zuzustimmen und diese Einwilligung jederzeit zu widerrufen. Diese ausdrückliche Einwilligung muss eine Willensbekundung sein, die frei, spezifisch und informiert durch eine klare Aussage oder affirmative Handlung erfolgt.[16]
6.1.2. Datenraumträgerschaften stellen sicher, dass es je nach Art der Daten und der Höhe des Risikos unterschiedliche Ebenen des Datenzugriffs und der Vertraulichkeit gibt.	6.2.2. Datenvermittelnde gewährleisten einfache Registrierungs- und Datennutzungsprozesse durch gängige Identifikationsmethoden (z.B. e-ID, Trust ID, Swiss-ID usw.).		6.4.2 Datenanbietende haben Zugang zu bestehenden Datensammlungen über ihr Profil/ihre Person und über Informationen zu Risiken der Zusammenführung von Daten in Datensammlungen, z.B. Profiling-Aktivitäten.[17]
6.1.3 Datenraumträgerschaften ermöglichen den Datenanbietenden jederzeit und mit einfachen Mitteln die Einwilligung sowie den Rückzug der Einwilligung zur Datennutzung.	6.2.3 Datenvermittelnde stellen sicher, dass bei Datennutzungen die Einwilligung der Datenanbietenden immer vorhanden ist.[18]	6.3.3 Datennutzende stellen sicher, dass bei Datennutzungen die Einwilligung der Datenanbietenden immer vorhanden ist.[19]	

15. *Betreffend besonders schützenswerten Personendaten i.S.v, Art. 5 lit.c DSG, betreffend Profiling mit hohem Risiko i.S.v. Art. 5 lit.g DSG, vgl. Art. 6 Abs. 7 DSG. Vgl. insb. auch Art. 31 sowie betreffend die Datenbearbeitung durch Bundesorgane, vgl. insb. Art. 33 ff. DSG.*
16. *Ibid.*
17. *Betreffend Personendaten i.S.v. Art. 5 lit. a DSG, vgl. insb. Art. 12, Art. 24 Abs. 4 DSG sowie Art. 6 Abs. 7 DSG und Art. 15 DSV betreffend Profiling.*
18. *Betreffend besonders schützenswerten Personendaten i.S.v. Art. 5 lit.c DSG, betreffend Profiling mit hohem Risiko i.S.v. Art. 5 lit.g DSG, vgl. Art. 6 Abs. 7 DSG.*
19. *Ibid.*

Empfehlung 7: Weitergabe
Sollte ein Datenraum die Weitergabe von Daten über den Datenraum hinaus vorsehen, so ist die Kontrolle über eine solche Weitergabe gewährleistet. Dies ist insbesondere der Fall, wenn es sich um Personendaten handelt.

Mögliche Umsetzungsmassnahmen zu Empfehlung 7

Datenraumträgerschaften	Datenvermittelnde	Datennutzende	Datenanbietende
7.1.1 Datenraumträgerschaften stellen sicher, dass die Weitergabe von Daten allgemein oder für eine bestimmte Verwendung jederzeit eingestellt werden kann. Das bedeutet, dass sie für Datenanbietende die Möglichkeit vorsehen müssen, die Einwilligung zu widerrufen, wodurch die weitere Nutzung der Daten untersagt wird.[20]	7.2.1 Datenvermittelnde sorgen für die Infrastruktur, damit die Weitergabe von Daten jederzeit eingestellt werden kann.		
7.1.2 Datenraumträgerschaften gewährleisten eine einfache Umsetzung der Löschung und/oder Vernichtung bestehender Daten, sodass diese Daten künftig nicht mehr verwendet werden können. Personendaten, welche zum Zweck der Bearbeitung nicht mehr erforderlich sind, müssen vernichtet oder anonymisiert werden.[21]	7.2.2 Auf Anfrage der Datenraumträgerschaften oder der Datenanbietenden löschen und/oder vernichten Datenvermittelnde die von der Anfrage betroffenen Daten und stellen sicher, dass diese nicht weitervermittelt werden.[22]	7.3.2 Auf Anfrage der Datenraumträgerschaften, der Datenvermittelnden oder der Datenanbietenden löschen und/oder vernichten Datennutzende die von der Anfrage betroffenen Daten und stellen sicher, dass diese nicht weiter genutzt werden.[23]	

20. *Dies gilt nur solange keine gesetzlichen Verpflichtungen bestehen, die betroffenen Daten weiterzugeben. Betreffend die erforderliche Einwilligung zur Bearbeitung von Personendaten, vgl. insb. Art. 6 Abs. 7 DSG.*
21. *Siehe Art.6, Abs. 4 DSG.*
22. *Personendaten i.S.v. Art. 5 lit. a DSG müssen gemäss Art. 6. Abs.4 DSG nicht erst auf Anfrage vernichtet oder anonymisiert werden, sondern bereits dann, wenn sie zum Zweck der Bearbeitung nicht mehr erforderlich sind.*
23. *Ibid.*

Empfehlung 8: Wahlfreiheit

Wo keine anderweitigen gesetzlichen Pflichten bestehen, ist die Teilnahme an einem Datenraum freiwillig.

Mögliche Umsetzungsmassnahmen zu Empfehlung 8

Datenraumträgerschaften	Datenvermittelnde	Datennutzende	Datenanbietende
8.1.1 Datenraumträgerschaften stellen sicher, dass Lock-In-Effekte mithilfe von technischen oder organisatorischen Vorkehrungen minimiert werden.	8.2.1 Datenvermittelnde ermöglichen die Datenportabilität.[24]	8.3.1 Datennutzende haben die freie Wahl, ob, und wenn ja, welchen Datenraum sie nutzen möchten.	8.4.1 Datenanbietende haben die freie Wahl ob, und wenn ja, in welchem Datenraum sie Daten bereitstellen möchten.
8.1.2 Datenraumträgerschaften ergreifen Massnahmen, um eine systematische und ungerechtfertigte Abhängigkeit von dominanten Akteuren (seien es externe Dienstleister, Datenanbietende oder Datennutzende) zu vermeiden, da diese Abhängigkeit den Datenaustausch erschweren oder unmöglich machen würde.			
		8.3.3 Datennutzende können die Übertragung ihrer Daten einfach ausführen.[25]	8.4.3 Datenanbietende können die Übertragung ihrer Daten einfach ausführen.[26]
8.1.4 Datenraumträgerschaften stellen sicher, dass Vertragsabschlüsse oder das Angebot von Dienstleistungen und Produkten (bspw. von Datenvermittelnden oder anderen für den Datenraum relevanten Dienstleistern) nicht von einer ungerechtfertigten Datenbereitstellung oder -nutzung abhängen.			

24. *Betreffend Personendaten i.S.v. Art. 5 lit. a DSG und Datenportabilität, vgl. insb. Art. 28-29 DSG.*
25. *Ibid.*
26. *Ibid.*

Empfehlung 9: Sicherheit
In einem Datenraum bestehen klare Prozesse, um Sicherheitsrisiken für den Datenraum und die beteiligten Akteure zu identifizieren und ggf. zu mindern.

Mögliche Umsetzungsmassnahmen zu Empfehlung 9

Datenraumträgerschaften	Datenvermittelnde	Datennutzende	Datenanbietende
9.1.1 Datenraumträgerschaften führen regelmässig Risikoevaluationen durch. Diese Evaluationen werden mit Massnahmen zur Verringerung der festgestellten Risiken ergänzt.			
9.1.2 Bei sensiblen Daten (d.h. besonders schützenswerten Personendaten oder wertvollen Sachdaten) führen Datenraumträgerschaften regelmässig eine externe Überprüfung der Risiken durch. Diese soll verschiedene Sicherheitsaspekte abdecken. [27]			
9.1.3 Datenraumträgerschaften definieren genaue Prozesse, wie vorzugehen ist, falls die bereitgestellten Daten kompromittiert werden sollten. Die Anweisungen umfassen einen definierten Plan für Notfallmassnahmen im Falle von Datenverlust oder Sicherheitslücken.	9.2.3 Datenvermittelnde befolgen die im Datenraum geltenden Notfallmassnahmen im Falle von Datenverlust oder Sicherheitslücken.	9.3.3 Datennutzende befolgen die im Datenraum geltenden Notfallmassnahmen im Falle von Datenverlust oder Sicherheitslücken.	9.4.3 Datenanbietende befolgen die im Datenraum geltenden Notfallmassnahmen im Falle von Datenverlust oder Sicherheitslücken.
	9.2.4 Bei Auffinden eines Datenverlusts oder einer Sicherheitslücke informieren Datenvermittelnde die betroffenen Parteien sofort, damit letztere geeignete Schutzmassnahmen ergreifen können.[28]	9.3.4 Bei Auffinden eines Datenverlusts oder einer Sicherheitslücke informieren Datennutzende die betroffenen Parteien sofort und in ausreichendem Masse, damit letztere geeignete Schutzmassnahmen ergreifen können.[29]	9.4.4 Bei Auffinden eines Datenverlusts oder einer Sicherheitslücke informieren Datenanbietende die betroffenen Parteien sofort, damit letztere geeignete Schutzmassnahmen ergreifen können.[30]
9.1.5 Wo immer möglich, fördern Datenraumträgerschaften den Gebrauch von automatischen Systemen zur Identifikation von Datenkopien und missbräuchlichen Nutzungsmustern. Resultate und Informationen aus diesen Systemen werden allen betroffenen Akteuren zur Verfügung gestellt.			

FAIRNESS

Empfehlung 10: Verhältnismässigkeit

Austausch, Nutzung und Mehrfachnutzung von Daten innerhalb eines Datenraums basieren auf dem Verhältnismässigkeitsprinzip.

Mögliche Umsetzungsmassnahmen zu Empfehlung 6

Datenraumträgerschaften	Datenvermittelnde	Datennutzende	Datenanbietende
10.1.1 Datenraumträgerschaften bestimmen die Bedingungen zur Teilnahme an einem Datenraum und kennen generell den Zweck der Datennutzung.	10.2.1 Datenvermittelnde fördern die Umsetzung milder Datennutzungsmethoden wie bspw. Anonymisierung, Pseudonymisierung, und Differential Privacy.[31]	10.3.1 Datennutzende stellen sicher, dass die Datennutzung innerhalb des Datenraums für den jeweiligen Zweck geeignet, erforderlich und zumutbar und mit den Bedingungen des Datenraums kompatibel ist.	10.4.1 Datenanbietende beachten bei der Datenerhebung, wo angezeigt, das Prinzip der Datenminimierung.[32]

27. *Betreffend Personendaten i.S.v. Art. 5 lit. a DSG besteht unter Art. 22 DSG die Pflicht zu einer Datenschutz-Folgenabschätzung wenn eine Bearbeitung ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen mit sich bringen kann.*
28. *Betreffend die Meldepflicht an den EDÖB, den Verantwortlichen oder die betroffene Person in Zusammenhang mit Verletzungen der Datensicherheit von Personendaten, vgl. insb. Art. 24 DSG und Art. 15 DSV.*
29. *Ibid.*
30. *Ibid.*
31. *Betreffend Personendaten i.S.v. Art. 5 lit. a DSG, vgl. Art. 7 DSG.*
32. *Ibid.*

Empfehlung 11: Diskriminierungsfreiheit
Datenraumspezifische Bedingungen und Betrieb eines Datenraums sind diskriminierungsfrei ausgestaltet und die Möglichkeit zur Teilnahme als Akteur ist nach sachlich objektiven Kriterien zu gewährleisten.

Mögliche Umsetzungsmassnahmen zu Empfehlung 11

Datenraumträgerschaften	Datenvermittelnde	Datennutzende	Datenanbietende
11.1.1 Datenraumträgerschaften stellen sicher, dass es nicht zu ungerechtfertigter Ungleichbehandlung von Akteuren betreffend den Zugang zu Datenräumen und innerhalb des Datenraums kommt.			
11.1.2 Datenraumträgerschaften identifizieren Hindernisse administrativer, wirtschaftlicher, technischer und sprachlicher Natur frühzeitig und treffen geeignete Massnahmen, um diese abzubauen.	11.2.2 Datenvermittelnde stellen für alle Akteure einen diskriminierungsfreien Zugang zum Datenraum sicher.		
11.1.3 Datenraumträgerschaften definieren objektive Kriterien für eine allfällige Ungleichbehandlung von Akteuren. Sie kommunizieren diese klar und informieren alle Akteure weshalb diese Kriterien eine Ungleichbehandlung rechtfertigen.		11.3.3 Datennutzende können bei Datenraumträgerschaften Informationen zu den Kriterien für eine allfällige Ungleichbehandlung einfordern.	11.4.3 Datenanbietende können bei Datenraumträgerschaften Informationen zu den Kriterien für eine allfällige Ungleichbehandlung einfordern.

Empfehlung 12: Interessenausgleich

Es besteht ein Interessenausgleich zwischen den Akteuren in einem Datenraum.

Mögliche Umsetzungsmassnahmen zu Empfehlung 12

Datenraumträgerschaften	Datenvermittelnde	Datennutzende	Datenanbietende
12.1.1 Datenraumträgerschaften definieren, wo immer möglich, gemeinsam in einem inklusiven Prozess mit den beteiligten Akteuren, wie und in welchem Masse Interessenausgleiche innerhalb des Datenraums vorgesehen sind.	12.2.1 Datenvermittelnde ermöglichen, sofern in den vereinbarten Bedingungen des Datenraums vorgesehen, einen Interessenausgleich zwischen Datennutzenden und Datenanbietenden (bspw. Monetarisierung, Kompensation seitens Datennutzenden) («Tauschgerechtigkeit im Sinne des individuellen Interesses»).	12.3.1 Datennutzende kompensieren, sofern in den vereinbarten Bedingungen des Datenraums vorgesehen, die Datenanbietenden.	12.4.1 Datenanbietende erhalten, sofern in den vereinbarten Bedingungen vorgesehen, eine Kompensation welche in einem angemessenen Verhältnis zu den angebotenen Daten steht.
12.1.2 Datenraumträgerschaften ermöglichen zur Sicherstellung des Interessenausgleichs - insbesondere von Individuen - transparente Repräsentationsverfahren oder andere wirksame Prozesse zur Berücksichtigung der Interessen aller Akteure und stellen ausreichende Ressourcen sicher.		12.3.2 Datennutzende machen die aus der Datennutzung gewonnenen Erkenntnisse, wenn immer möglich, in standardisierter Form allgemein verfügbar («Tauschgerechtigkeit im Sinne des öffentlichen Interesses»).	12.4.2 Datenanbietende können bei der Datenraumträgerschaft Stellungnahmen abgeben oder zu den Kriterien für den Interessenausgleich bei den Datenraumträgerschaften Informationen einfordern.

Empfehlung 13: Datenqualität
Alle Akteure innerhalb eines Datenraums streben eine hohe Datenqualität an. Daten haben direkte Auswirkungen auf die Gestaltung von Produkten und Dienstleistungen. Entsprechend können qualitativ unzulängliche Datensätze zu Diskriminierung und Ungleichbehandlungen führen.

Mögliche Umsetzungsmassnahmen zu Empfehlung 13

Datenraumträgerschaften	Datenvermittelnde	Datennutzende	Datenanbietende
13.1.1 Datenraumträgerschaften (oder allenfalls Datenvermittelnde) definieren klare Leitfäden zu den nötigen Qualitätsanforderungen der zur Verfügung gestellten Daten und den Anforderungen bezüglich Transparenz und Informationen, falls die Datenqualität reduziert sein sollte.	13.2.1 Datenvermittelnde (oder allenfalls Datenraumträgerschaften) definieren klare Leitfäden zu den nötigen Qualitätsanforderungen der zur Verfügung gestellten Daten und den Anforderungen bezüglich Transparenz und Informationen, falls die Datenqualität reduziert sein sollte.	13.3.1 Datennutzende informieren Datenraumträgerschaft und Datenvermittelnde über mögliche Verbesserungen der Leitfäden aus Perspektive der Datennutzenden.	13.4.1 Datenanbietende setzen die für den Datenraum definierten Qualitätsanforderung der zur Verfügung gestellten Daten konsequent um.
13.1.2 Datenraumträgerschaften fördern das Verständnis aller Akteure innerhalb eines Datenraums für die Bedeutung einer hohen Datenqualität.	13.2.2 Datenvermittelnde ermöglichen Datennutzenden und Datenanbietenden Informationen über die Datenqualität auszutauschen und allfällige Unzulänglichkeiten zu melden.	13.3.2 Datennutzende melden den Datenanbietenden (oder, falls dies nicht möglich ist, den Datenvermittelnden), wenn sie innerhalb eines Datensatzes nicht deklarierte Unzulänglichkeiten oder eingeschränkte Qualität identifizieren. Bei Personendaten bestehen gesetzliche Pflichten zur Datenrichtigkeit.[33]	13.4.2 Datenanbietende deklarieren Qualitätsmängel, nicht-repräsentative Datensätze sowie mögliche daraus resultierende Datenverzerrungen klar und transparent. Wo möglich, unternehmen sie die nötigen Anstrengungen, um diese zu beheben. Bei Personendaten bestehen gesetzliche Pflichten zur Datenrichtigkeit.[34]
13.1.3 Datenraumträgerschaften identifizieren geeignete Prozesse und setzen diese ein, um die Datenqualität und die Datenrepräsentativität zu fördern.			13.4.3 Datenanbietende reagieren prompt auf Meldungen von unzulänglichen Datensätzen. Wo möglich, verbessern sie den fraglichen Datensatz. Ansonsten deklarieren sie die Unzulänglichkeiten klar und transparent.
13.1.4 Datenraumträgerschaften (oder allenfalls die Datenvermittelnden) treffen mit Datenanbietenden klare Vereinbarungen zur Datenpflege, welche für die Datenanbietenden verpflichtend sind.	13.2.4 Datenvermittelnde (oder allenfalls Datenraumträgerschaften) treffen mit Datenanbietenden klare Vereinbarungen zur Datenpflege, welche für die Datenanbietenden verpflichtend sind.		13.4.4 Datenanbietende verfügen über ein klares Verständnis bezüglich ihrer Pflichten zur Datenpflege.

33. *Betreffend Personendaten i.S.v. Art. 5 lit. a DSG, vgl. Art. 6 Abs. 5 DSG. Vgl. insb. auch Art. 32 und Art. 41 DSG.*

34. *Ibid.*

Empfehlung 14: Besonderer Schutz von Kindern und Jugendlichen
Kinder und Jugendliche geniessen aufgrund der geringen Erfahrung besonderen Schutz, wenn sie an einem Datenraum teilnehmen.

Mögliche Umsetzungsmassnahmen zu Empfehlung 14

Datenraumträgerschaften	Datenvermittelnde	Datennutzende	Datenanbietende
14.1.1 Datenraumträgerschaften definieren bei der Teilnahme von Kindern und Jugendlichen im Datenraum besondere Schutzmassnahmen. Diese müssen insbesondere folgende Umstände berücksichtigen: das Alter des Kindes, die Urteilsfähigkeit, die Art der bearbeiteten Daten, den Zweck der Bearbeitung sowie die spezifischen Risiken der Bearbeitung personenbezogener Daten von Kindern und Jugendlichen.	14.2.1 Datenvermittelnde stellen die Einhaltung besonderer Schutzmassnahmen gegenüber Kindern und Jugendlichen sicher.		

EFFEKTIVITÄT

Empfehlung 15: Umsetzung

Der in einem Datenraum geltende Gouvernanzrahmen wird effektiv angewendet und umgesetzt.

Mögliche Umsetzungsmassnahmen zu Empfehlung 15

Datenraumträgerschaften	Datenvermittelnde	Datennutzende	Datenanbietende
15.1.1 Datenraumträgerschaften definieren und kommunizieren klare Massnahmen betreffend Nichteinhaltung der vereinbarten Verantwortlichkeiten.	15.2.1 Datenvermittelnde setzen die von den Datenraumträgerschaften definierten Massnahmen bei Nichteinhaltung der vereinbarten Verantwortlichkeiten um.	15.3.1 Datennutzende setzen die von den Datenraumträgerschaften definierten Massnahmen bei Nichteinhaltung der vereinbarten Verantwortlichkeiten um.	15.4.1 Datenanbietende setzen die von den Datenraumträgerschaften definierten Massnahmen bei Nichteinhaltung der vereinbarten Verantwortlichkeiten um.
15.1.2 Datenraumträgerschaften etablieren oder definieren Beschwerdestellen, an welche sich Akteure im Konfliktfall wenden können. Diese Beschwerdestellen erfüllen Verfahrensgarantien zur Wahrung eines ordnungsgemässen Verfahrens und der Verfahrensgerechtigkeit.			
15.1.3 Datenraumträgerschaften informieren die betroffenen Akteure betreffend einschlägiger Rechtsbehelfe.			
15.1.4 Datenraumträgerschaften sehen für alle beteiligten Datenraumakteure zugängliche Evaluationsmechanismen vor, um die Wirksamkeit der bestehenden Gouvernanz regelmässig zu beurteilen.			

Empfehlung 16: Interoperabilität
Alle Akteure fördern die Interoperabilität von Datenräumen.

Mögliche Umsetzungsmassnahmen zu Empfehlung 16

Datenraumträgerschaften	Datenvermittelnde	Datennutzende	Datenanbietende
16.1.1 Datenraumträgerschaften stellen die Interoperabilität des Datenraums in rechtlicher und organisatorischer Sicht sicher.	16.2.1 Datenvermittelnde stellen die Interoperabilität des Datenraums in technischer und semantischer Hinsicht sicher.	16.3.1 Datennutzende halten sich an die Interoperabilitätsvorgaben von Datenraumträgerschaften und Datenvermittelnden.	16.4.1 Datenanbietende halten sich an die Interoperabilitätsvorgaben von Datenraumträgerschaften und Datenvermittelnden.
16.1.2 Datenraumträgerschaften bestimmen relevante Standards mit Bedacht und in Absprache mit allen involvierten Stakeholdern. Diese Standards sind in klaren Leitfäden definiert und einfach zugänglich und verständlich.	16.2.2 Datenvermittelnde bestimmen relevante Standards mit Bedacht und in Absprache mit allen involvierten Stakeholdern. Diese Standards sind in klaren Leitfäden definiert und einfach zugänglich und verständlich.	16.3.2 Datennutzende nutzen die zur Verfügung gestellten Leitfäden und halten sich an die im Datenraum geltenden Standards.	16.4.2 Datenanbietende nutzen die zur Verfügung gestellten Leitfäden und halten sich an die im Datenraum geltenden Standards.
16.1.3 Datenraumträgerschaften prüfen, ob sich bereits bestehende offene Standards eignen und übernehmen solche, wann immer möglich, um die Kompatibilität mit anderen Datenräumen zu erhöhen.	16.2.3 Datenvermittelnde prüfen, ob sich bereits bestehende, offene Standards eignen und übernehmen solche, wann immer möglich, um die Kompatibilität mit anderen Datenräumen zu erhöhen.		
16.1.4 Datenraumträgerschaften fördern offene und gemeinsame Standards, insbesondere innerhalb eines spezifischen Sektors.	16.2.4 Datenvermittelnde fördern offene und gemeinsame Standards, insbesondere innerhalb eines spezifischen Sektors.		

Empfehlung 17: Agilität
Datenräume entwickeln sich kontinuierlich weiter und können sich veränderten Gegebenheiten schnell und flexibel anpassen.

Mögliche Umsetzungsmassnahmen zu Empfehlung 17

Datenraumträgerschaften	Datenvermittelnde	Datennutzende	Datenanbietende
17.1.1 Datenraumträgerschaften wählen die Infrastruktur, Form und das Geschäftsmodell eines Datenraums bewusst und in Abwägung zukünftiger Entwicklungen.			
17.1.2 Datenraumträgerschaften legen die Organisations- und Gouvernanzstrukturen so an, dass sie auch bei sich rasch verändernden Gegebenheiten funktionsfähig bleiben und in angemessener Zeit angepasst werden können. Zu diesem Zweck werden Feedback-Mechanismen eingerichtet.	17.2.2 Datenvermittelnde bringen sich in den Entwicklungsprozess des Datenraums bestmöglich via Feedback-Mechanismen ein.	17.3.2 Datennutzende bringen sich in den Entwicklungsprozess des Datenraums bestmöglich via Feedback-Mechanismen ein.	17.4.2 Datenanbietende bringen sich in den Entwicklungsprozess des Datenraums bestmöglich via Feedback-Mechanismen ein.

Empfehlung 18: Nachhaltigkeit
Alle Akteure setzen sich für die ökologische, soziale und wirtschaftliche Nachhaltigkeit des Datenraums ein.

Mögliche Umsetzungsmassnahmen zu Empfehlung 18

Datenraumträgerschaften	Datenvermittelnde	Datennutzende	Datenanbietende
18.1.1 Datenraumträgerschaften führen regelmässige Folgenabschätzungen bezüglich der Nachhaltigkeit des Datenraums durch.			
18.1.2 Datenraumträgerschaften identifizieren, basierend auf diesen Folgenabschätzungen, Risiken und entwickeln konkrete Massnahmen zu deren Reduktion und Minimisierung.	18.2.2 Datenvermittelnde setzen Massnahmen zur Risikoreduktion bestmöglich um.	18.3.2 Datennutzende setzen Massnahmen zur Risikoreduktion bestmöglich um.	18.4.2 Datenanbietende setzen Massnahmen zur Risikoreduktion bestmöglich um.