

DATENAUSWERTEPLATTFORM (§ 11 DES GESUNDHEITS-ZIELSTEUERUNGSGESETZES)

Die folgende Datenschutz-Folgenabschätzung (DSFA) betrifft die Datenauswerteplattform gemäß § 11 des Gesundheit-Zielsteuerungsgesetzes (G-ZG) in Verbindung mit den Bestimmungen des Gesundheits- und Sozialbereichs im Sinne des Art. 9 Abs. 2 Buchstabe h DSGVO. Eine demonstrative, aber dennoch detaillierte Liste dieser Bestimmungen findet sich unten im Feld „BEWERTUNG / Rechtmäßigkeit der Verarbeitung“.

Wesentlich für das Feststellen einer Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung ist die Auslegung von Art. 35 DSGVO, wie sie insbesondere durch die Art 29-Datenschutzgruppe (dem Vorgängergremium des Europäischen Datenschutzausschusses) ergangen ist (*Art-29-Datenschutzgruppe*, Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt“ WP 248 Rev.01).

Eine Datenschutz-Folgenabschätzung ist gemäß Art. 35 Abs. 3 Buchstabe b DSGVO erforderlich, weil es zu einer Verarbeitung

- in großem Umfang (WP 248, 11),
- von sensiblen Daten sowie
- darüber hinaus Daten zu schutzbedürftigen Betroffenen, wie etwa Patient:innen oder in einem Abhängigkeitsverhältnis zu den Trägern der Sozialversicherung stehenden Gesundheitsdiensteanbietern (WP 248, 12)

kommt.

Außerdem ist die Datenschutz-Folgenabschätzung angezeigt, um das Risiko von erfolgreichen Schadenersatzverfahren gemäß Art. 82 DSGVO für die Verantwortlichen größtmöglich zu senken. Zwar hat der Europäische Gerichtshof im Mai 2023 festgestellt, dass die Verletzung von Bestimmungen der DSGVO für die Zuerkennung von Schadenersatz alleine nicht ausreicht und es daher unbedingt des Nachweises eines Schadens bedarf. Gleichzeitig hat er aber auch festgestellt, dass es keine Erheblichkeitsschwelle für die Geltendmachung immaterieller Schäden gibt (EuGH 4.5.2023, C-300/21 Rn. 51). Die dieser Datenschutz-Folgenabschätzung zugrundeliegenden Ermächtigungen zur Steuerung des Gesundheitswesens (in § 11 G-ZG) sind daher auch ganz stark vor dem Hintergrund zu sehen, jegliche Zweifel über die Rechtmäßigkeit dieser Verarbeitungen auszuräumen und Schadenersatzansprüche bereits aus diesem Grund hintanzuhalten (vgl. *Reimer/Stanonik*, Risk-Management in Zeiten des [verschuldensunabhängigen] immateriellen Schadenersatzes, dako 5/2023, 106 [109]). Aufgrund des Anwendungsvorrangs der DSGVO können Haftungsansprüche selbst bei gesetzlich vorgesehenen Verarbeitungen nicht ausgeschlossen werden, allerdings ist davon auszugehen, dass allfällige Verstöße gegen das nationale Determinierungsgebot (Art. 18 B-VG bzw. § 1 DSG) keine Haftung gemäß Art. 82 DSGVO zu begründen vermögen, weil Art. 82 DSGVO nur Verstöße gegen die DSGVO sanktioniert (*Reimer/Stanonik*, Fn 32 und 33) und die DSGVO durch den Verweis auf das „Recht des Mitgliedstaats“ u.a. in Art. 9 Abs. 2 Buchstabe h DSGVO keine Bestimmung hinsichtlich der Rechtsform trifft, diese somit nicht harmonisiert. Bis zur Aufhebung durch den Gesetzgeber oder den VfGH existiert daher das „Recht eines Mitgliedstaats“ und solange es nicht – beispielsweise wegen Verstoßes gegen das Datenminimierungsprinzip im Sinne des Art. 5 Abs. 1 Buchstabe c DSGVO – unangewendet bleiben muss, legitimiert es daher auch darauf beruhende Verarbeitungen.

Die Voraussetzungen für den Entfall gemäß Art. 35 Abs. 10 DSGVO sind nicht gegeben, weil nicht bloß Daten gemäß Art. 6 Abs. 1 Buchstabe c oder e DSGVO, sondern Daten gemäß Art. 9 DSGVO verarbeitet werden sollen. Die vorliegende Datenschutz-Folgenabschätzung soll aber als so genannte Referenz-DSFA (WP 248, 8) öffentlich zugänglich gemacht werden und allen Verantwortlichen (im Sinne des Art. 26 DSGVO) die Einhaltung von Art. 35 DSGVO erleichtern bzw. die Qualität von § 11 G-ZG in der vorgeschlagenen Fassung verbessern.

Zusammengefasst hat die vorliegenden Datenschutz-Folgenabschätzung folgendes Ergebnis gebracht:

Beschreibung	Bewertung	Risiken	Abhilfemaßnahmen	DS-Interessen
Art der Verarbeitung	festgelegter Zweck	Schäden	Minimierung	Datenschutzbeauftragter
Umfang der Verarbeitung	eindeutiger Zweck	Kontrollverlust	Pseudonymisierung	betroffene Personen
Kontext der Verarbeitung	legitimer Zwecke	Diskriminierung	Transparenz	
Zweck der Verarbeitung	Rechtmäßigkeit	Identitätsdiebstahl & -betrug	Überwachung	
personenbezogene Daten	Angemessenheit	Finanzielle Verluste	Datensicherheitsmaßnahmen	
Empfänger:innen	Erheblichkeit	unbef Aufhebung Pseudonymisierung		
Speicherdauer	Beschränktheit auf notwendiges Maß	Rufschädigung		
funktionelle Beschreibung	Speicherbegrenzung	Verlust Berufsgeheimnisse		
Hard- und Software	generelle Informationen	gesellschaftliche Nachteile		
Verhaltensregeln	Informationen (Art 13 DSGVO)	(Risiken bei Unterbleiben)		
	Informationen (Art 14 DSGVO)			
	Auskunft & Datenübertragbarkeit			
	Berichtigung & Löschung			
	Widerspruch & Einschränkung			
	Auftragsverarbeiter:innen		Legende	erfüllt
	Übermittlung in Drittländer			erfüllbar
	vorherige Konsultation			nicht erfüllt

<p>SYSTEMATISCHE BESCHREIBUNG der geplanten Verarbeitungsvorgänge, Zwecke sowie berechtigten Interessen</p> <p><i>Die Beschreibung hat nach Erwägungsgrund 90 sowie Art. 35 Abs. 7 Buchstabe a und Abs. 8 DSGVO sowie den Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt“ der Artikel-29-Datenschutzgruppe (WP 248) zu enthalten:</i></p>	
<p>Art der Verarbeitung (EG 90 DSGVO; WP 248 Rev.01, 21 und 28)</p>	<p>Die Verarbeitung erfolgt elektronisch im Rahmen einer Server-Client-Applikation.</p> <p>Aus Gründen der Datensicherheit gemäß Art. 32 DSGVO unterbleibt an dieser Stelle eine genaue Beschreibung der technischen Umsetzung, um potentielle Angreifer:innen nicht mit wertvollen Informationen über potentielle Schwachstellen (<i>Art-29-Datenschutzgruppe</i>, WP 248 Rev.01, 8) zu versorgen.</p> <p>Verantwortliche im Sinne des Art. 4 Nr. 7 DSGVO sind die Zielsteuerungspartner gemäß § 11 Abs. 1 G-ZG, d.h. der Bund, die Länder sowie der Dachverband der Sozialversicherungsträger und die ihm angehörenden Sozialversicherungsträger, die die Plattform als gemeinsam Verantwortliche im Sinne des Art. 26 DSGVO einzurichten und zu betreiben haben. Durch § 11 Abs. 1 G-ZG wird die besondere Art der Verarbeitung gesetzlich näher determiniert (vgl. VfSlg. 18.643/2008, wonach eine besondere Art der Verarbeitung, wie etwa von videogestützten Geschwindigkeits- und Abstandsmesssystemen, einer ausdrücklichen, gesetzlichen Ermächtigung bedarf). Die Bezeichnung als Plattform sowie die Löschfrist gemäß § 11 Abs. 4 Z 4 G-ZG erlauben eine vorübergehende, zentrale Verarbeitung.</p> <p>Die Anforderung “Beschreibung der Art der Verarbeitung” ist aufgrund der angeführten Beschreibung als erfüllt anzusehen.</p>
<p>Umfang der Verarbeitung (EG 90 DSGVO; WP 248 Rev.01, 21 und 28)</p>	<p>Die Datenauswerteplattform umfasst potenziell alle Personen, die mit dem österreichischen Gesundheitswesen – egal in welcher Rolle – in Berührung kommen.</p> <p>In inhaltlicher Sicht umfasst die Datenauswerteplattform Primärdaten im Sinne des § 3 Z 9 G-ZG (siehe näher zum Begriff der Primärdaten, unten Feld „BESCHREIBUNG / Personenbezogene Daten“).</p> <p>In geografischer Sicht umfasst die Datenauswerteplattform das gesamte Bundesgebiet, weil die evidenzbasierte Planung und Steuerung des österreichischen Gesundheitswesens ermöglicht werden soll. Die Datenauswerteplattform stellt bereits aufgrund des geographischen Ausmaßes einen großen Umfang im Sinne der Art-29-Datenschutzgruppe (WP 248, 11) dar.</p> <p>Die Anforderung “Beschreibung des Umfangs der Verarbeitung” ist aufgrund der angeführten Beschreibung als erfüllt anzusehen.</p>
<p>Kontext der Verarbeitung (EG 90 DSGVO; WP 248 Rev.01, 21 und 28)</p>	<p>Die Verarbeitung erfolgt im Kontext der Planung und Steuerung des österreichischen Gesundheitssystems, genauer gesagt der Vollziehung von Gesetzen im Gesundheits- und Sozialbereich gemäß Art. 9 Abs. 2 Buchstabe h DSGVO (zur rechtlichen Begründung – siehe unten: Feld „BEWERTUNG / Rechtsgrundlage“).</p> <p>Die Anforderung “Beschreibung des Kontexts der Verarbeitung” ist aufgrund der angeführten Beschreibung als erfüllt anzusehen.</p>
<p>Zweck der Verarbeitung (EG 90 sowie Art. 35 Abs. 7 Buchstabe a DSGVO; WP 248 Rev.01, 21 und 28)</p>	<p>Die Verarbeitung dient primär der Einhaltung des verfassungsrechtlichen Effizienzgebotes (Art. 51 Abs. 8 B-VG bzw. VfSlg. 14.500/1996) beim Einsatz öffentlicher Mittel sowie der Einhaltung des verfassungsrechtlichen Grundgedankens der Verantwortlichkeit oberster Organe (VfSlg. 3054/1956).</p>

	<p>Zu deren Einhaltung müssen die obersten Organe, d.h. u.a. auch die Gesundheitsminister:in, effektiv Steuerungs- und Lenkungenfunktionen wahrnehmen; können sie dies nicht, sind entgegenstehende einfachgesetzliche Bestimmungen verfassungswidrig (VfSlg. 17.421/2004). Zur Wahrnehmung der Steuerungs- und Lenkungenfunktionen bedarf es Informationen. Einfachgesetzliche Bestimmungen, die die „<i>umfassende und rechtzeitige Information des Bundesministers nicht sichern</i>“ (VfSlg. 16.400/2001), beschränken in verfassungswidriger Weise die Leitungs- und Organisationsverantwortung der dem Parlament gegenüber gemäß Art. 76 B-VG verantwortlichen Bundesminister:innen (VfSlg. 16.400/2001). Wenn die entsprechende Steuerungsmöglichkeit nicht besteht, die neben Weisungsrechten vorab Informationsrechte bedingt, liegt ein Verstoß gegen das Organisationskonzept der Bundesverfassung, wie es insbesondere in den Art. 20 Abs. 1 und Art. 77 B-VG zum Ausdruck kommt, vor (VfSlg. 19.728/2012).</p> <p>Nach Erwägungsgrund 32 DSGVO können Verarbeitungen auch mehreren Zwecken dienen. Dies ist im gegebenen Zusammenhang der Fall, da die Datenauswertepattform</p> <ul style="list-style-type: none"> ▪ der Steuerung des Gesundheitswesens (§ 11 Abs. 2 Z 1 G-ZG), ▪ der Evaluierung von gesundheitspolitischen und Public Health-Aktivitäten (§ 11 Abs. 2 Z 2 G-ZG), ▪ der Qualitätssicherung (§ 11 Abs. 2 Z 3 G-ZG), ▪ der Implementierung, Durchführung und Beobachtung der partnerschaftlichen Zielsteuerung-Gesundheit (§ 11 Abs. 2 Z 4 G-ZG) sowie ▪ dem Management außergewöhnlicher Ereignisse, wie etwa Epidemien und Pandemien (§ 11 Abs. 2 Z 5 G-ZG) <p>dient.</p> <p>Die Anforderung „Beschreibung des Zwecks der Verarbeitung“ ist aufgrund der angeführten Beschreibung als erfüllt anzusehen.</p>
<p>Personenbezogene Daten (WP 248 Rev.01, 21 und 28)</p>	<p>Der Personenbezug ist iSd Art. 4 Nr. 1 DSGVO weit zu verstehen, sodass nicht nur Informationen, die sich auf bereits identifizierte Personen, sondern auch Informationen, die sich auf identifizierbare natürliche Personen beziehen, davon umfasst sind.</p> <p>Wesentlicher Anknüpfungspunkt zur Feststellung des Umfangs der personenbezogenen Daten sind</p> <ul style="list-style-type: none"> ▪ die Definition der Primärdaten (§ 3 Z 9 G-ZG), ▪ die Gegenüberstellung von Primärdaten und Auswertungen (§ 11 Abs. 4 Z 3 und 4 G-ZG) sowie ▪ der Verweis auf Betriebs- und Vollziehungskennzahlen („<i>Nutzungen, die aufgrund einer gesetzlichen Verpflichtung in Übereinstimmung mit Art. 6 oder 9 DSGVO vorgesehen sind</i>“ gemäß § 11 Abs. 6 Z 4 G-ZG). <p>Unter Primärdaten sind alle im Gesundheits- oder Sozialbereich (Art. 9 Abs. 2 lit. h DSGVO) angefallenen und anfallenden Verwaltungsdaten (§ 3 Z 17 des Bundesstatistikgesetzes 2000, BGBl. I Nr. 163/1999), wie etwa Daten aus dem eHealth-Verzeichnisdienst oder anderen bei Stellen im Gesundheits- oder Sozialbereich verarbeiteten Daten, sowie aufgrund des Zusatzes „(Daten aus dem extra- und intramuralen)“ auch bei Gesundheitsdiensteanbieter:innen (§ 2 Z 2 GTelG 2012) verarbeitete Daten. Die Primärdaten gehen daher über Gesundheitsdaten im Sinne des Art. 4 Nr. 15 DSGVO hinaus, weil auch Daten, aus denen keine Informationen über den Gesundheitszustand von betroffenen Personen hervorgehen, davon umfasst sein können, weil sie zur Erreichung der Zwecke gemäß § 11 Abs. 2 G-ZG erforderlich sind, wie beispielsweise die schon zuvor genannten Verwaltungsdaten. Wichtig ist in diesem Zusammenhang anzumerken, dass es sich bei den Primärdaten um personenbezogene Daten im Sinne des Art. 4 Nr. 1 DSGVO handeln kann, aber nicht muss.</p>

Auswertungen werden auf Basis der Primärdaten erstellt (§ 11 Abs. 3 G-ZG), sind somit von diesen zu unterscheiden. Ein prominentes und bereits zum aktuellen Zeitpunkt detailliert ausgearbeitetes Beispiel für eine mögliche zukünftige Auswertung der Datenauswertungsplattform stellt die so genannte Betriebskennzahlendatenbank von ELGA dar. Weitere Auswertungen könnten sein:

- Analysen zur sektorübergreifenden Versorgung und den Gesundheits-Outcomes von Menschen mit chronischen Krankheiten (z.B. Diabetes)
- sektorenübergreifende Analyse von Patientenströmen etwa in Abhängigkeit der regionalen Versorgung oder des regionalen Krankheitsgeschehens
- Evaluation von gesundheitspolitischen und sonstigen gesundheitsrelevanten Maßnahmen
- Gesundheitspersonalbedarfsprognosen
- Analysen zum über den höchsten Bildungsabschluss angenäherten sozio-ökonomischen Status von bestimmten Patientenpopulationen

Die angeführten Auswertungen könnten wie folgt aussehen:

- Betriebskennzahlendatenbank gemäß Gesundheitstelematikgesetz 2012:
 - Daten betreffend die Gesundheitsdiensteanbieter:innen (inkl. Adresse)¹
 - Daten zur Situation des (technischen) Behandlungskontaktes sowie der Methode der Patient:innenidentifikation²
 - Daten zu den Transaktionen elektronischer Befunde³
 - Daten zu den Transaktionen der eMedikation⁴
 - Daten zu den Impf-Transaktionen⁵
 - Daten zu ZPI-Transaktionen⁶
 - Daten zum Cross Community Access (XCA)⁷
 - Daten zur Nutzung der individuellen ELGA-Teilnehmer:innenrechte⁸ (PAP)⁹
 - Angaben zum Vollständigkeitsstand des GDA-Index¹⁰
 - Daten zu Transaktionen des GDA-Index¹¹
 - Angaben zum Vollständigkeitsstand des ZPI¹²
 - Daten zu Transaktionen des ZPI¹³
 - Auswertungen zu den in der eMedikation gespeicherten elektronischen Medikationsdaten¹⁴
 - Auswertungen zu den elektronischen Medikationslisten¹⁵
 - Auswertungen zu den in ELGA-Bereichen gespeicherten Befunden¹⁶

¹ ELGA GmbH, Betriebskennzahlen Lastenheft V1.0, Zeilen 2 ff. Diese Daten stammen aus dem GDA-Index.

² ELGA GmbH, Betriebskennzahlen Lastenheft V1.0, Zeilen 29 ff.

³ ELGA GmbH, Betriebskennzahlen Lastenheft V1.0, Zeilen 42 ff. Der Personenbezug ergibt sich aus der Verarbeitung der GDA-OIDs, die bei Ärzt:innen – im Wege des öffentlichen OID-Portals – auf die hinter den OIDs stehenden natürlichen Personen rückführbar sind. Das öffentliche OID-Portal ist unter https://www.gesundheit.gv.at/OID_Frontend/index.jsp?section=1 allgemein einsehbar.

⁴ ELGA GmbH, Betriebskennzahlen Lastenheft V1.0, Zeilen 55 ff.

⁵ ELGA GmbH, Betriebskennzahlen Lastenheft V1.0, Zeilen 100 ff. Der Personenbezug ergibt sich aus der Verarbeitung der GDA-OID.

⁶ ELGA GmbH, Betriebskennzahlen Lastenheft V1.0, Zeilen 108 ff. Der Personenbezug ergibt sich aus der Verarbeitung der GDA-OID.

⁷ ELGA GmbH, Betriebskennzahlen Lastenheft V1.0, Zeilen 182 ff. Der Personenbezug ergibt sich aus der Verarbeitung der GDA-OID.

⁸ § 15 Abs. 2 und § 16 GTelG 2012.

⁹ ELGA GmbH, Betriebskennzahlen Lastenheft V1.0, Zeilen 201 ff.

¹⁰ ELGA GmbH, Betriebskennzahlen Lastenheft V1.0, Zeilen 217 ff.

¹¹ ELGA GmbH, Betriebskennzahlen Lastenheft V1.0, Zeilen 265 ff.

¹² ELGA GmbH, Betriebskennzahlen Lastenheft V1.0, Zeilen 207 ff.

¹³ ELGA GmbH, Betriebskennzahlen Lastenheft V1.0, Zeilen 251 ff.

¹⁴ ELGA GmbH, Betriebskennzahlen Lastenheft V1.0, Zeilen 55 ff. Der Personenbezug ergibt sich aus der Verarbeitung der GDA-OID.

¹⁵ ELGA GmbH, Betriebskennzahlen Lastenheft V1.0, Zeilen 81 ff.

¹⁶ ELGA GmbH, Betriebskennzahlen Lastenheft V1.0, Zeilen 238 ff. Ein möglicher Personenbezug kann sich – vor dem Hintergrund der Judikatur zur Mindestgruppengröße von 6 (DSB 30.3.2015, DSB-D215.611/0003-

- Auswertungen zu den elektronischen Bildern¹⁷
- Auswertungen zu Impfdaten¹⁸
- Daten zu den Transaktionen betreffend das Zugangsportal¹⁹
- Daten zum CDA-Validator²⁰
- Bedeutungsliste²¹
- Daten betreffend die Krankenanstalten²²
- Daten zu den ELGA-Bereichen²³
- Daten aus dem System der leistungsorientierten Krankenanstaltenfinanzierung²⁴

Wenn die mittels Auswertungen festgestellten Betriebs- und Vollziehungskennzahlen beispielsweise einen schlechten Vollständigkeitsstand des ZPI ergeben, können nun nähere Untersuchungen zu den Ursachen angestellt werden und diese – beispielsweise im Zuge einer zukünftigen Novelle – beseitigt werden. Die Auswertungen können auch als Bündel von Betriebs- und Vollziehungskennzahlen bezeichnet werden.

Die „Nutzungen, die aufgrund einer gesetzlichen Verpflichtung in Übereinstimmung mit Art. 6 oder 9 DSGVO vorgesehen sind“ (§ 11 Abs. 6 Z 4 G-ZG) stellen im Wesentlichen **Betriebs- und Vollziehungskennzahlen** zu den jeweiligen Materiengesetzen dar. Dass es sich um Materiengesetze handelt, ergibt sich aus der Definition der Primärdaten in § 3 Z 9 G-ZG, die auf den Gesundheits- und Sozialbereich im Sinne des Art. 9 Abs. 2 Buchstabe h DSGVO verweist. Eine demonstrative Liste solcher Materiengesetze findet sich unten im Feld „BEWERTUNG / Rechtmäßigkeit der Verarbeitung“. Eine grundlegende (verfassungs-)gesetzliche Verpflichtung der obersten Organe, besteht gemäß Art. 20 Abs. 1 B-VG in der Führung des ihnen – im Falle der Bundesminister:innen insbesondere durch das Bundesministeriengesetz 1986 (BMG) – zugewiesenen Verwaltungsbereichs, d.h. insbesondere der Vollziehung der Materiengesetze für die sie aufgrund des Bundesministeriengesetzes 1986 zuständig sind. Wenn nun das Beispiel der Betriebskennzahlendatenbank herangezogen wird, wäre

- die Pflicht der Gesundheitsminister:in gemäß § 19 GTelG 2012 zur Führung des GDA-Index die *gesetzliche Verpflichtung*;
- die Pflicht der Gesundheitsminister:in zur wirkungsorientierten Vollziehung gemäß Art. 51 B-VG oder zur Einhaltung der Gesetze gemäß Art. 18 B-VG in Bezug § 19 GTelG 2012 das Interesse der Gesundheitsminister:in an der *Nutzung* (der Primärdaten) *in Übereinstimmung mit Art. 6 oder 9 DSGVO*, weil
 - bei nichtsensiblen Daten, die jeweilige verfassungsrechtliche Anforderung in Verbindung mit § 19 GTelG 2012 eine rechtliche Verpflichtung gemäß Art. 6 Abs. 1 Buchstabe c darstellt oder
 - bei sensiblen Daten, die jeweilige verfassungsrechtliche Anforderung in Verbindung mit § 19 GTelG 2012 sowie § 11 G-ZG das Recht eines Mitgliedstaats im Sinne des Art. 9 Abs. 2 beispielsweise Buchstabe g, h oder i DSGVO darstellt;
- die Angabe zum Vollständigkeitsstand des GDA-Index eine zur Kontrolle der gesetzlichen Verpflichtung des § 19 GTelG 2012 geeignete *Betriebs- oder Vollziehungskennzahl*.

DSB/2014; DSK 22.5.2013, K213.180/0021-DSK/2013) – auch hinsichtlich der Gruppenpraxen ergeben, weil es durchaus sein kann, dass es befundschreibende Gruppenpraxen mit weniger als 6 Ärzt:innen gibt.

¹⁷ ELGA GmbH, Betriebskennzahlen Lastenheft V1.0, Zeilen 88 ff. Der Personenbezug ergibt sich aus der Verarbeitung der GDA-OID.

¹⁸ ELGA GmbH, Betriebskennzahlen Lastenheft V1.0, Zeilen 108 ff. Der Personenbezug ergibt sich aus der Verarbeitung der GDA-OID.

¹⁹ ELGA GmbH, Betriebskennzahlen Lastenheft V1.0, Zeilen 123 ff.

²⁰ ELGA GmbH, Betriebskennzahlen Lastenheft V1.0, Zeilen 199 f.

²¹ ELGA GmbH, Betriebskennzahlen Lastenheft V1.0, Zeilen 229 ff.

²² ELGA GmbH, Betriebskennzahlen Lastenheft V1.0, Zeilen 146 ff.

²³ ELGA GmbH, Betriebskennzahlen Lastenheft V1.0, Zeilen 189 ff.

²⁴ ELGA GmbH, Betriebskennzahlen Lastenheft V1.0, Zeilen 161 ff.

Betriebs- und Vollziehungskennzahlen knüpfen somit immer an einer gesetzlichen Verpflichtung an: sie haben eine juristische Seite, die sich oft auch auf eine Kombination (verfassungs-)gesetzlicher Verpflichtungen stützen wird und eine wirtschaftliche Seite, die im Sinne des Controllings eine zahlenmäßige Darstellung der Erfüllung dieser (verfassungs-)gesetzlichen Verpflichtungen ist.

Um auf das Beispiel der Verpflichtung gemäß § 19 GTelG 2012 zurückzukommen: Das Wissen, darum wie die Pflicht gemäß § 19 GTelG 2012 tatsächlich erfüllt wird, ist nicht nur für die Gesundheitsminister:in selbst, sondern beispielsweise auch für die Länder erforderlich, wenn diese ihre Impfprogramme gemäß § 24f Abs. 4 Z 4 in Verbindung mit § 24f Abs. 2 sowie § 19 GTelG 2012 abrechnen und ihrerseits beispielsweise wieder landes-(verfassungs-)gesetzlichen Verpflichtungen unterliegen.

Für die Gesundheitsminister:in ist die Betriebs- oder Vollziehungskennzahl zu § 19 GTelG 2012 zudem u.a. für die Ausarbeitung sachlicher, legislativer Entwürfe erforderlich: Neben den reinen Vollziehungsaufgaben stellt die Ausarbeitung von Regierungsvorlagen nämlich eine der wesentlichen Aufgaben eines obersten Organs (des Bundes) dar (§ 3 Abs. 1 Z 2 BMG). Um den Regelungsbedarf in sachlicher Art und Weise feststellen zu können, müssen zumindest die (bisherige) Vollziehungspraxis sowie die zu regelnden Sachverhalte bekannt sein. Beides lässt sich in den angeführten Betriebs- und Vollziehungskennzahlen beschreiben. Auch wenn grundsätzlich jede materiengesetzliche Aufgabe mit einer oder mehreren Betriebs- und Vollziehungskennzahlen versehen werden kann und daher für die betroffenen Personen anhand der Materiengesetze vorhersehbar ist, stellt die genaue Definition dieser Betriebs- und Vollziehungskennzahlen eine der zentralen Aufgaben des Gremiums gemäß § 11 Abs. 6 Z 1 und 3 bis 5 G-ZG dar. Diese Vorarbeiten des Gremiums können von der Gesundheitsminister:in für die nähere Definition im Rahmen einer Verordnung gemäß § 11 Abs. 7 G-ZG herangezogen werden. Eine (nochmalige) gesetzliche Regelung (der Grundlagen) solcher Betriebs- und Vollziehungskennzahlen (etwa in den Materiengesetzen) ist nicht nur nicht erforderlich (näher dazu die Entscheidung EGMR 09.01.2018, RS0125045 sowie die Entscheidungen der Datenschutzbehörde zum Bundesministerengesetz 1986 – siehe unten: Feld „BEWERTUNG / Rechtmäßigkeit der Verarbeitung“), sondern sogar kontraproduktiv und zwar aus folgendem Grund: auch wenn Verweise auf andere Bestimmungen, insbesondere von Personen ohne juristische Ausbildung als schwer verständlich abgelehnt werden, tragen Verweise doch wesentlich zur Rechtssicherheit bei. Durch die Anknüpfung an eine andere Bestimmung wird die Idee eines *single point of truth* in die juristische Welt übertragen. Mit der Verdoppelung oder Vervielfachung von Regelungsinhalten wird die Gefahr von unbeabsichtigten Widersprüchen und Seiteneffekten wesentlich erhöht. Dieses Problem zeigt sich eindrucksvoll am Beispiel der Vollziehungsklauseln: das Bundesministerengesetz stellt eine aktuelle, allgemeine Regelung dar. Die speziellen Vollziehungsklauseln oder Ressortbezeichnungen in den Materiengesetzen werden oft (nicht zeitnahe) nachgezogen, sodass es zu unbeabsichtigten Widersprüchen käme, gäbe es nicht die Sonderbestimmung des § 17 BMG, die genau dieses Problem adressiert und abweichend von der *lex specialis*-Regelung, sogar die Legalfiktion der Novellierung durch das Bundesministerengesetz 1986 ausdrücklich anordnet. Mit dem Erfordernis einer zusätzlichen, gesetzlichen Regelung für jedes Materiengesetz würde dieses Problem auch für die oben angeführten Betriebs- und Vollziehungskennzahlen geschaffen werden. Besser insbesondere im Sinne der Vorhersehbarkeit des Eingriffs ist daher die allgemeine, gesetzliche Regelung durch § 11 G-ZG kombiniert mit einer allfälligen Konkretisierung der Datenarten auf – im Sinne des Stufenbaus der Rechtsordnung – untergeordneter Ebene durch eine Verordnung gemäß § 11 Abs. 7 G-ZG, weil damit allfällige Widersprüche einfacher erkenn- und lösbar sind: wenn sich die Materiengesetze ändern, sind auch allenfalls darauf

	<p>aufbauende Verordnungen gemäß § 11 Abs. 7 G-ZG zu ändern bzw. mangels entsprechender Novellierung (klar) gesetzwidrig.</p> <p>Die Anforderung “Beschreibung der personenbezogenen Daten” ist aufgrund des in § 11 G-ZG geregelten „Betriebs- und Vollziehungskennzahlen“ jedenfalls als erfüllbar anzusehen.</p>
<p>Empfänger:innen (EG 90 DSGVO; WP 248 Rev.01, 21 und 28)</p>	<p>Der Austausch von Primärdaten ist nur zwischen den Zielsteuerungspartnern zulässig (§ 11 Abs. 3 und Abs. 4 Z 3 G-ZG). Darüber hinaus dürfen Primärdaten nicht übermittelt werden. Auswertungen unterliegen hingegen keinen Übermittlungsbeschränkungen, weil es sich weder um personenbezogene Daten im Sinne des Art. 4 Nr. 1 DSGVO noch um Primärdaten handelt. Sie dürfen daher veröffentlicht werden.</p> <p>Wissenschaftlichen Einrichtungen im Sinne des § 2b Z 13 des Forschungsorganisationsgesetzes ist es – theoretisch wie anderen Personen oder Institutionen auch – unbenommen, bei Gesundheits-Zielsteuerungspartnern Auswertungen zu bestimmten Betriebs- und Vollziehungskennzahlen anzuregen. Ein Recht darauf besteht nicht; unter Umständen können diese externen Anregungen allerdings den Gesundheits-Zielsteuerungspartnern bei der Verbesserung der Vollziehung helfen, weil sie relevante Auswertungen anregen und somit – nach Entscheidung durch den jeweiligen Gesundheits-Zielsteuerungspartner – ermöglichen. Zulässige Empfänger:innen sind darüber hinaus gemäß Art. 28 DSGVO herangezogene Auftragsverarbeiter:innen der Gesundheits-Zielsteuerungspartner.</p> <p>Um wissenschaftlichen Einrichtungen im Sinne des § 2b Z 13 des Forschungsorganisationsgesetzes oder § 31 des Bundesstatistikgesetzes 2000 Zugang zu in der Datenauswertungsplattform verarbeiteten pseudonymisierten Daten zu gewähren, können die Möglichkeiten im Forschungsorganisationsgesetz (§ 2d in Verbindung mit § 38b FOG) oder der §§ 31ff des Bundesstatistikgesetzes 2000 sowie in zukünftigen unionsrechtlichen Regelungen, etwa im Rahmen des Europäischen Gesundheitsdatenraumes, genutzt werden. Denkbar sind auch Freigaben gemäß § 11 Abs. 6 Z 5 G-ZG.</p> <p>Die Anforderung “Beschreibung der Empfänger:innen” ist aufgrund der angeführten Beschreibung als erfüllt anzusehen.</p>
<p>Speicherdauer (WP 248 Rev.01, 21 und 28)</p>	<p>Eine Mindestspeicherdauer ist gesetzlich nicht vorgesehen. Die Löschrfrist ist in § 11 Abs. 4 Z 4 G-ZG so angegeben, dass die abgeholten Primärdaten nach der Erstellung der angeforderten Auswertungen zu löschen sind. Auf die Verwendung des Wortes „unverzüglich“ oder „sofort“ wurde im Gesetzgebungsprozess bewusst verzichtet, sodass die Löschung jedenfalls zeitnahe zu erfolgen hat, aber einer Nachfrage beim beauftragenden Gesundheits-Zielsteuerungspartner, ob die angeforderte Auswertung, den Anforderungen entspricht, nicht entgegensteht.</p> <p>Die Löschrpflicht des § 11 Abs. 4 Z 4 G-ZG sorgt also dafür, dass die Datenauswertungsplattform nicht zu einem Datenfriedhof wird. Sollten Daten zu einem späteren Zeitpunkt – aufgrund einer neuerlichen Anforderung eines Gesundheits-Zielsteuerungspartners – wieder benötigt werden, dürfen die erforderlichen Primärdaten erneut angefordert werden. Die Löschrpflicht des § 11 Abs. 4 Z 4 G-ZG bezieht sich nur auf die Datenauswertungsplattform sowie die Primärdaten. Sollten die Gesundheits-Zielsteuerungspartner unmittelbar die Bereitstellung von Primärdaten beantragen (dieses Recht steht ihnen gemäß § 11 Abs. 3 G-ZG zu), richten sich deren Speicher- bzw. Löschrfristen nach ihren speziellen, rechtlichen Anforderungen. Nachdem es sich dann um eine Verarbeitung außerhalb der hier gegenständlichen gemeinsamen Verarbeitung handelt, liegt die Verantwortlichkeit für derartige Verarbeitungen ausschließlich bei den betreffenden Gesundheits-Zielsteuerungspartnern. Nicht umfasst von der Löschrpflicht sind außerdem die – ebenfalls gemäß § 11 Abs. 3 G-ZG – bereitzustellenden Metadaten und Dokumentationen.</p>

	<p>Die Anforderung “Beschreibung der Speicherdauer” ist aufgrund der angeführten Beschreibung als erfüllt anzusehen.</p>
<p>Funktionelle Beschreibung der Verarbeitungsvorgänge (WP 248 Rev.01, 21 und 28)</p>	<p>Die Datenauswerteplattform umfasst folgende Funktionen:</p> <ul style="list-style-type: none"> ▪ Primärdaten abholen: Mittels Abfrage werden die Primärdaten von den Gesundheits-Zielsteuerungspartnern elektronisch angefordert. Entsprechend den gemäß § 11 Abs. 7 Z 1, 2 und 4 G-ZG vorgeschriebenen Service Level Agreements sind die Gesundheits-Zielsteuerungspartner gemäß § 11 Abs 3 G-ZG zur automatisierten Bereitstellung von Primärdaten – etwa im Wege von REST-APIs – verpflichtet. Die inhaltliche Aufbereitung dieser verordneten SLAs ist in § 11 Abs. 6 Z 1 G-ZG vorgesehen und eine der zentralen Aufgaben des Gremiums gemäß § 11 Abs. 5 G-ZG. ▪ Primärdaten temporär speichern: Zur Erstellung von Auswertungen dürfen die abgeholten Primärdaten vorübergehend – d.h. bis zur Erstellung der angeforderten Auswertung – gespeichert werden. ▪ Auswertung erstellen: Für die in § 11 Abs. 2 G-ZG beschriebenen Zwecke, insbesondere der Planung, Steuerung und zur Sicherstellung einer gesamthaften Finanzierung des österreichischen Gesundheitswesens können Auswertungen erstellt werden. Vor der Freigabe von Auswertungen ist über die so genannte k-Anonymität (für $k > 5$) sicherzustellen, dass den Anforderungen des § 11 Abs. 4 Z 3 G-ZG sowie der Datenschutzbehörde (DSB 30.03.2015, DSB-D215.611/0003-DSB/2014; DSK 22.05.2013, K213.180/0021-DSK/2013) an datenschutzkonforme Statistiken entsprochen wird. ▪ Primärdaten löschen: Die abgeholten Primärdaten können – aus technischer Sicht – jederzeit gelöscht werden. Nach der Erstellung von Auswertungen sind diese jedenfalls zu löschen. <p>Die Anforderung “Funktionelle Beschreibung der Verarbeitungsvorgänge” ist aufgrund der angeführten Beschreibung als erfüllt anzusehen.</p>
<p>Beschreibung der Hard- und Software bzw. sonstigen Infrastruktur (WP 248 Rev.01, 21 und 28)</p>	<p>Da die Datenauswerteplattform noch zu errichten ist (§ 11 Abs. 1 G-ZG), sind hinsichtlich der genauen Beschreibung der Infrastruktur noch allfällige Ausschreibungen abzuwarten.</p> <p>Die Anforderung “Beschreibung der Hard- und Software bzw. sonstigen Infrastruktur” ist aufgrund der angeführten Beschreibung als erfüllbar anzusehen.</p>
<p>Eingehaltene, gemäß Art. 40 DSGVO genehmigte Verhaltensregeln (Art. 35 Abs. 8 DSGVO; WP 248 Rev.01, 21 und 28)</p>	<p>Das Instrument der Verhaltensregeln ist für Behörden und öffentliche Stellen nicht anwendbar (Art. 41 Abs. 6 DSGVO bzw. mwN <i>Schweinoch/Will</i> in <i>Ehmann/Selmayr</i>, DSGVO² Art. 40-43 Rn. 10). Da die Datenauswerteplattform allerdings von erheblichem öffentlichen Interesse ist (näher dazu – siehe unten: BEWERTUNG / Rechtmäßigkeit der Verarbeitung) sollen als Folge dieser Datenschutz-Folgenabschätzung verwaltungsinterne Erlässe und Rundschreiben für die öffentlich-rechtlichen Gesundheits-Zielsteuerungspartner sowie allgemeine verfügbare Datenschutzinformationen, wie etwa die Datenschutzerklärung, aktualisiert bzw. ausgearbeitet werden.</p> <p>Die Anforderung “Beschreibung der eingehaltenen, gemäß Art 40 genehmigten Verhaltensregeln” ist aufgrund der angeführten Beschreibung als erfüllbar anzusehen.</p>
<p>BEWERTUNG der Notwendigkeit und Verhältnismäßigkeit</p> <p><i>Die Bewertung hat nach Erwägungsgründen 90 und 96, Art. 35 Abs. 7 Buchstaben b und d DSGVO sowie den Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung</i></p>	

im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt“ (WP 248) auf Maßnahmen
 – betreffend Notwendigkeit und Verhältnismäßigkeit (Art. 5 und 6 DSGVO) sowie
 – zur Stärkung der Rechte der betroffenen Personen (Art. 12 bis 21, 28, 36 und Kapitel V DSGVO) abzustellen.

<p>Festgelegter Zweck (EG 90 und Art. 35 Abs. 7 Buchstabe b DSGVO; WP 248 Rev.01, 21 und 28)</p>	<p>Die Zwecke der Verarbeitung sind in § 11 Abs. 2 G-ZG wie folgt festgelegt:</p> <ul style="list-style-type: none"> ▪ Steuerung von Struktur, Organisation, Qualität und Finanzierung der österreichischen Gesundheitsversorgung (§ 11 Abs. 2 Z 1 G-ZG), ▪ Evaluierung von gesundheitspolitischen und Public Health Aktivitäten (§ 11 Abs. 2 Z 2 G-ZG), ▪ Sicherstellung eines funktionierenden, flächendeckenden und sektorenübergreifenden Qualitätssystems in Österreich (§ 11 Abs. 2 Z 3 G-ZG), ▪ Implementierung, Durchführung und Beobachtung der partnerschaftlichen Zielsteuerung-Gesundheit (§ 11 Abs. 2 Z 4 G-ZG) sowie ▪ Management von außergewöhnlichen Ereignissen wie beispielsweise Pandemien und Epidemien (§ 11 Abs. 2 Z 5 G-ZG). <p>Die Anforderung “Bewertung der Festlegung des Zwecks” ist aufgrund der ausdrücklichen, gesetzlichen Festlegung des Zwecks in § 11 Abs. 2 des Gesundheits-Zielsteuerungsgesetzes als erfüllt anzusehen.</p>
<p>Eindeutiger Zweck (Art. 35 Abs. 7 Buchstabe b iVm Art. 5 Abs. 1 Buchstabe b DSGVO; WP 248 Rev.01, 21 und 28)</p>	<p>Die Zwecke sind in § 11 Abs. 2 G-ZG eindeutig festgelegt. In Zusammenschau mit den jeweiligen Materiengesetzes des Gesundheits- und Sozialbereichs können betroffene Personen vorhersehen, wie ihre Daten verarbeitet werden.</p> <p>Die Anforderung “Bewertung der Eindeutigkeit des Zwecks” ist aufgrund der ausdrücklichen, gesetzlichen Festlegung des Zwecks in § 11 Abs. 2 des Gesundheits-Zielsteuerungsgesetzes als erfüllt anzusehen.</p>
<p>Legitimer Zweck (Art. 35 Abs. 7 Buchstabe b iVm Art. 5 Abs. 1 Buchstabe b DSGVO; WP 248 Rev.01, 21 und 28)</p>	<p>Die eindeutig festgelegten Zwecke sind zudem legitim. Dies zeigt sich bereits auf unionsrechtlicher Ebene: danach steht gemäß Art. 168 Abs. 7 AEUV die Verantwortung für die Festlegung ihrer Gesundheitspolitik sowie für die Organisation des Gesundheitswesens und der medizinischen Versorgung den Mitgliedstaaten zu. Dies umfasst auch die Verwaltung des Gesundheitswesens und der medizinischen Versorgung sowie die Zuweisung der dafür bereitgestellten Mittel. Auf verfassungsrechtlicher Ebene ergibt sich die Legitimität der Zwecke vor allem aus Art. 10 Abs. 1 Z 10 B-VG, wonach dem Bund die – grundsätzliche – Kompetenz im Gesundheitswesen zukommt. Es gibt somit einen klaren verfassungsrechtlichen Gestaltungsauftrag hinsichtlich des Gesundheitswesens.</p> <p>Die Verantwortlichkeit der obersten Organe stellt einen „Grundgedanken der Verfassung“ dar (VfSlg. 3054/1956). Zu deren Einhaltung müssen die obersten Organe, d.h. u.a. auch die Gesundheitsminister:in effektiv Steuerungs- und Lenkungenfunktionen wahrnehmen; kann sie dies nicht, sind entgegenstehende einfachgesetzliche Bestimmungen verfassungswidrig (VfSlg. 17.421/2004). Dazu bedarf es Informationen. Einfachgesetzliche Bestimmungen, die die „umfassende und rechtzeitige Information des Bundesministers nicht sichern“ (VfSlg. 16.400/2001), beschränken in verfassungswidriger Weise die Leitungs- und Organisationsverantwortung der dem Parlament gegenüber gemäß Art. 76 B-VG verantwortlichen Bundesminister:innen (VfSlg. 16.400/2001). Mit (verfassungs-)gesetzlich übertragenen Aufgaben ist – nach Ansicht des VfGH – jedenfalls auch die entsprechende Verarbeitungsbefugnis verbunden, weil andernfalls die übertragene Aufgabe nicht erfüllt werden könnte (VfSlg. 15.130/1998). In diesem Sinn hat auch der Europäische Gerichtshof – zuletzt Anfang 2019 – das Vorliegen einer rechtlichen Verpflichtung gemäß Art. 7 Buchstabe a DSRL bzw. Art. 6 Abs. 1 Buchstabe c DSGVO hinsichtlich zollrechtlicher Genehmigungsvoraussetzungen (Durchführungsverordnung [EU] 2015/2447 der Kommission vom 24. November 2015 mit Einzelheiten zur Umsetzung</p>

	<p>von Bestimmungen der Verordnung [EU] Nr. 952/2013 des Europäischen Parlaments und des Rates zur Festlegung des Zollkodex der Union, ABl. Nr. L 343 vom 29.12.2015, S. 558.) bejaht. Dazu führte der EuGH in seiner Entscheidung C-496/17 „Deutsche Post“ vom 16. Jänner 2019 in Randnummer 61 Folgendes aus:</p> <p><i>„Die anschließende Erhebung dieser personenbezogenen Daten durch die Zollbehörden zwecks Bescheidung eines Antrags auf Bewilligung des AEO-Status erscheint notwendig, um eine rechtliche Verpflichtung zu erfüllen, der diese Behörden nach Art. 24 Abs. 1 Unterabs. 2 der Durchführungsverordnung 2015/2447 unterliegen, und um die Voraussetzungen einzuhalten, die darin für die Bewilligung dieses Status aufgestellt werden. Insofern werden diese Daten für festgelegte, eindeutige und legitime Zwecke erhoben und somit verarbeitet.“</i></p> <p>Die vom EuGH zitierte Bestimmung des Art. 24 Abs. 1 Unterabs. 2 der Durchführungsverordnung 2015/2447 lautet:</p> <p><i>„Ist der Antragsteller keine natürliche Person, gilt die Voraussetzung des Artikels 39 Buchstabe a des Zollkodex als erfüllt, wenn keine der folgenden Personen in den letzten drei Jahren einen schwerwiegenden Verstoß oder wiederholte Verstöße gegen die zoll- oder steuerrechtlichen Vorschriften oder eine schwere Straftat im Rahmen ihrer Wirtschaftstätigkeit begangen hat:</i></p> <p><i>a) der Antragsteller;</i></p> <p><i>b) die Person, die für das antragstellende Unternehmen verantwortlich ist oder die Kontrolle über seine Leitung ausübt;</i></p> <p><i>c) der Beschäftigte des Antragstellers, der für dessen Zollangelegenheiten zuständig ist.“</i></p> <p>Da Art. 24 Abs. 1 Unterabs. 2 der Durchführungsverordnung 2015/2447 auch auf „schwere Straftaten“ abstellt, sind von der Ermächtigung jedenfalls auch Daten im Sinne des Art. 10 DSGVO erfasst. Diese sind aufgrund der gemeinsamen Nennung in Art. 35 Abs. 3 Buchstabe b DSGVO – zumindest für Zwecke von Datenschutz-Folgenabschätzungen – als gleichrangig anzusehen, sodass die aus der Entscheidung C-496/17 zu ziehenden Schlüsse auch auf Daten gemäß Art. 9 angewandt werden können.</p> <p>Die Anforderung „Bewertung der Legitimität des Zwecks“ ist aufgrund des Art. 168 Abs. 7 AEUV, des Art. 10 Abs. 1 Z 10 B-VG, der ausdrücklichen, gesetzlichen Regelung in § 11 des Gesundheits-Zielsteuerungsgesetzes sowie im Lichte der einschlägigen EuGH- und VfGH-Judikatur, als erfüllt anzusehen.</p>
<p>Rechtmäßigkeit der Verarbeitung <small>(Art. 35 Abs. 7 Buchstabe b iVm Art. 6 und 9 DSGVO; WP 248 Rev.01, 21 und 28)</small></p>	<p>Die Rechtmäßigkeit der Verarbeitung ergibt sich aus Art. 6 Abs. 1 Buchstabe c und e sowie Art. 9 Abs. 2 Buchstaben g, h und i DSGVO, weil die Verarbeitung erforderlich für die Steuerung des Gesundheitswesens ist. Dabei handelt es sich um eine Aufgabe, die im öffentlichen Interesse liegt, das nach Ansicht der Datenschutzbehörde</p> <ul style="list-style-type: none"> ▪ zum einen bereits dann vorliegt, wenn die bessere Planung von medizinischen Vorsorgemaßnahmen bloß ermöglicht wird (DSK 21.08.2001, K202.007/004-DSK/2001) und ▪ zum anderen sogar erheblich ist – und damit auch zur Verarbeitung sensibler Daten berechtigt –, wenn <ul style="list-style-type: none"> – die Rechtsordnung dem Thema in mehrfacher Hinsicht, d.h. durch Regelung an unterschiedlichen Stellen, einen hohen Stellenwert einräumt (DSK 07.09.2006, K202.047/0009-DSK/2006), – die angestrebten Ergebnisse nicht vorhanden sind (DSK 07.09.2006, K202.047/0009-DSK/2006) und – konkrete Finanzierungs- bzw. Unterstützungszusagen von zumindest drei mit dem Thema befassten staatlichen bzw.

staatlich finanzierten Einrichtungen vorliegen
(DSK 07.09.2006, K202.047/0009-DSK/2006).

Sämtliche Voraussetzungen der datenschutzrechtlichen Judikatur zum Vorliegen eines erheblichen öffentlichen Interesses (DSK 07.09.2006, K202.047/0009-DSK/2006) sind erfüllt, weil

- es eine Vielzahl einschlägiger Steuerungsbestimmungen gibt, d.h. die Rechtsordnung dem Thema in mehrfacher Hinsicht einen hohen Stellenwert einräumt;
- die angestrebten Ergebnisse nicht vorhanden sind (vgl. *Degelsegger-Márquez/Gruböck/Fidon*, Gesundheitsdaten in Österreich – ein Überblick – Ergebnisbericht [2022]);
- konkrete Finanzierungs- bzw. Unterstützungszusagen – etwa in Form der Einigung der Gesundheits-Zielsteuerungspartner, d.h. mehr als drei mit dem Thema befassten staatlichen Einrichtungen, vorliegen.

Der Auftrag zur Steuerung ergibt sich aus einer **Vielzahl einschlägiger Steuerungsbestimmungen**, wie insbesondere:

- Art. 51 Abs. 8 und Abs. 9 Z 1 B-VG, die den Grundsatz der Wirkungsorientierung auf verfassungsrechtlicher Ebene in Österreich vorsehen. Der Grundsatz der Wirkungsorientierung bedeutet, dass bei Budgeterstellung und Haushaltsführung eine Orientierung an den mit den eingesetzten Mitteln erreichten Wirkungen erfolgt. Im Zusammenhang mit der Wirkungsorientierung ist auch eine angemessene Evaluierung der Ziele vorzunehmen, wobei die mit der Evaluierung entstehenden Kosten in einem vertretbaren Verhältnis zum Nutzen der Evaluierungen stehen sollen (ErläutRV 203 BlgNR 23. GP 8).
Bei den Maßnahmen für eine wirkungsorientierte Verwaltung wird es darauf ankommen, die Verknüpfung von Ergebnis- und Ressourcenverantwortung unter Nutzung internationaler Erfahrungen so vorzunehmen, dass diese in effizienter, unbürokratischer Weise umgesetzt wird. Die zugrunde liegende Absicht muss stets handlungsleitend bleiben, nämlich die Steuerung der eingesetzten Mittel nach beabsichtigten Wirkungen und Leistungen mit einem vertretbaren Verwaltungsaufwand vorzunehmen und Verantwortlichen in Politik und Verwaltung aussagekräftige und ohne unzumutbaren Aufwand verarbeitbare Informationen zur Hand zu geben, die diese Verantwortlichen für ihre Steuerungsaufgaben benötigen und die gleichzeitig einer breiten, interessierten Öffentlichkeit deutlich machen, welche Zusammenhänge zwischen eingesetzten Mitteln und Wirkungen/Leistungen bestehen (ErläutRV 203 BlgNR 23. GP 9).
- Art. 51 Abs. 8 B-VG, der die Effizienz als einen der Grundsätze der Haushaltsführung des Bundes auf verfassungsrechtlicher Ebene vorsieht. Es ist anzustreben, dass auch Länder und Gemeinden diese Grundsätze bei ihrer Haushaltsführung anwenden (ErläutRV 203 BlgNR 23. GP 8).
- § 11 des AIDS-Gesetzes 1993, wonach die Gesundheitsminister:in mit der Vollziehung des AIDS-Gesetzes 1993 betraut ist.
- § 69 des Apothekengesetzes, wonach die Gesundheitsminister:in mit der Vollziehung des Apothekengesetzes betraut ist.
- § 82 Z 2 des Apothekenkammergesetzes 2001 in Verbindung mit Teil 2 lit. L Z 11 der Anlage zu § 2 des Bundesministeriengesetzes 1986, wonach die Gesundheitsminister:in mit der Vollziehung des Apothekenkammergesetzes 2001 betraut ist.
- § 9 des Arzneibuchgesetzes 2012, wonach die Gesundheitsminister:in mit der Vollziehung des Arzneibuchgesetzes 2012 betraut ist.
- § 96 Abs. 1 des Arzneimittelgesetzes, wonach die Gesundheitsminister:in mit der Vollziehung des Arzneimittelgesetzes betraut ist.
- § 2 des Arzneiwareneinfuhrgesetzes 2002 in Verbindung mit Teil 2 lit. L Z 9 der Anlage zu § 2 des Bundesministeriengesetzes 1986, wonach die Gesundheitsminister:in mit der Vollziehung des Arzneiwareneinfuhrgesetzes 2002 betraut ist.

- § 27 des Arzneiwareneinführungsgesetzes 2010, wonach die Gesundheitsminister:in mit der Vollziehung des Arzneiwareneinführungsgesetzes 2010 betraut ist.
- § 218 Abs. 1 Z 2 des Ärztegesetzes 1998, wonach – grundsätzlich – die Gesundheitsminister:in mit der Vollziehung des Ärztegesetzes 1998 betraut ist.
- § 19 Z 2 des Bäderhygienegesetzes, wonach – grundsätzlich – die Gesundheitsminister:in mit der Vollziehung des Bäderhygienegesetzes betraut ist.
- § 26 des Blutsicherheitsgesetzes 1999, wonach – grundsätzlich – die Gesundheitsminister:in mit der Vollziehung des Bäderhygienegesetzes betraut ist.
- § 26 Abs. 1 des Bundesgesetzes über die Gesundheit Österreich GmbH, wonach – grundsätzlich – die Gesundheitsminister:in mit der Vollziehung des Bundesgesetzes über die Gesundheit Österreich GmbH betraut ist.
- § 13 des Bundesgesetzes über die Dokumentation im Gesundheitswesen, wonach – grundsätzlich – die Gesundheitsminister:in mit der Vollziehung des Bundesgesetzes über die Dokumentation im Gesundheitswesen betraut ist.
- § 14 des Bundesgesetzes über die Durchführung von ästhetischen Behandlungen und Operationen, wonach – grundsätzlich – die Gesundheitsminister:in mit der Vollziehung des Bundesgesetzes über die Durchführung von ästhetischen Behandlungen und Operationen betraut ist.
- § 16 des eEltern-Kind-Pass-Gesetzes (der zwar noch nicht in Kraft getreten ist, aber zukünftig die Vollziehung des eEltern-Kind-Pass-Gesetzes der Gesundheitsminister:in übertragen wird), wonach – grundsätzlich – die Gesundheitsminister:in mit der Vollziehung des eEltern-Kind-Pass-Gesetzes betraut sein wird.
- § 51 des Epidemiegengesetzes 1950, wonach – grundsätzlich – die Gesundheitsminister:in mit der Vollziehung des Epidemiegengesetzes 1950 betraut ist.
- § 22 des EU-Qualitätsregelungen-Durchführungsgesetzes, wonach – grundsätzlich – die Gesundheitsminister:in mit der Vollziehung des EU-Qualitätsregelungen-Durchführungsgesetzes betraut ist.
- § 13 des EWR-Psychologengesetzes, wonach die Gesundheitsminister:in mit der Vollziehung des EWR-Psychologengesetzes betraut ist.
- § 13 des EWR-Psychotherapiengesetzes, wonach die Gesundheitsminister:in mit der Vollziehung des EWR-Psychotherapiengesetzes betraut ist.
- § 76 des Gehaltskassengesetzes 2002 in Verbindung mit Teil 2 lit. L Z 11 der Anlage zu § 2 des Bundesministeriengesetzes 1986, wonach die Gesundheitsminister:in mit der Vollziehung des Gehaltskassengesetzes 2002 betraut ist.
- § 111 des Gentechnikgesetzes, wonach – grundsätzlich – die Gesundheitsminister:in mit der Vollziehung des Gentechnikgesetzes betraut ist.
- § 16 des Geschlechtskrankheitengesetzes in Verbindung mit Teil 2 lit. L Z 9 der Anlage zu § 2 des Bundesministeriengesetzes 1986, wonach die Gesundheitsminister:in mit der Vollziehung des Geschlechtskrankheitengesetzes betraut ist.
- § 20 des Gesundheits- und Ernährungssicherheitsgesetzes, wonach – grundsätzlich – die Gesundheitsminister:in mit der Vollziehung des Gesundheits- und Ernährungssicherheitsgesetzes betraut ist.
- § 118 des Gesundheits- und Krankenpflegegesetzes, wonach – grundsätzlich – die Gesundheitsminister:in mit der Vollziehung des Gesundheits- und Krankenpflegegesetzes betraut ist.
- § 30 des Gesundheitsberuferegister-Gesetzes, wonach die Gesundheitsminister:in mit der Vollziehung des Gesundheitsberuferegister-Gesetzes betraut ist.
- § 5 Abs. 1 des Gesundheitsförderungsgesetzes, wonach – mit Ausnahme dessen § 4 – die Gesundheitsminister:in mit der Vollziehung des Gesundheitsförderungsgesetzes betraut ist.

- § 11 Abs. 1 des Gesundheitsqualitätsgesetzes, wonach die Gesundheitsminister:in mit der Vollziehung des Gesundheitsqualitätsgesetzes betraut ist.
- § 31 des Gesundheitstelematikgesetzes 2012, wonach die Gesundheitsminister:in mit der Vollziehung des Gesundheitstelematikgesetzes 2012 betraut ist.
- § 40 des Gesundheits-Zielsteuerungsgesetzes, wonach – grundsätzlich – die Gesundheitsminister:in mit der Vollziehung des Gesundheits-Zielsteuerungsgesetzes betraut ist.
- § 39 des Gewebesicherheitsgesetzes, wonach die Gesundheitsminister:in mit der Vollziehung des Gewebesicherheitsgesetzes betraut ist.
- § 63 des Hebammengesetzes, wonach – grundsätzlich – die Gesundheitsminister:in mit der Vollziehung des Hebammengesetzes betraut ist.
- § 25 des Heimaufenthaltsgesetzes, wonach – teilweise – die Gesundheitsminister:in mit der Vollziehung des Heimaufenthaltsgesetzes betraut ist.
- § 10 des Impfschadengesetzes, wonach – teilweise – die Gesundheitsminister:in mit der Vollziehung des Impfschadengesetzes betraut ist.
- § 37 des Kardiotechnikergesetzes, wonach – grundsätzlich – die Gesundheitsminister:in mit der Vollziehung des Kardiotechnikergesetzes betraut ist.
- § 67 Abs. 2 des Bundesgesetzes über Krankenanstalten und Kuranstalten, wonach – grundsätzlich – die Gesundheitsminister:in mit der Vollziehung des Bundesgesetzes über Krankenanstalten und Kuranstalten betraut ist.
- § 4 des KRAZAF-Abwicklungsgesetzes, wonach die Gesundheitsminister:in mit der Vollziehung des KRAZAF-Abwicklungsgesetzes betraut ist.
- § 5 des Krebsstatistikgesetzes in Verbindung mit Teil 2 lit. L Z 9 der Anlage zu § 2 des Bundesministeriengesetzes 1986, wonach die Gesundheitsminister:in mit der Vollziehung des Krebsstatistikgesetzes betraut ist.
- § 67 Abs. 2 des Bundesgesetzes über Krankenanstalten und Kuranstalten, wonach – grundsätzlich – die Gesundheitsminister:in mit der Vollziehung des Bundesgesetzes über Krankenanstalten und Kuranstalten betraut ist.
- § 107 des Lebensmittelsicherheits- und Verbraucherschutzgesetzes, wonach – grundsätzlich – die Gesundheitsminister:in mit der Vollziehung des Lebensmittelsicherheits- und Verbraucherschutzgesetzes betraut ist.
- § 17 in Verbindung mit Teil 2 lit. L Z 9 der Anlage zu § 2 des Bundesministeriengesetzes 1986, wonach die Gesundheitsminister:in mit der Vollziehung der Verordnung betreffend Leichen von mit anzeigepflichtigen Krankheiten behafteten Personen betraut ist.
- § 43 des Medizinische Assistenzberufe-Gesetzes, wonach die Gesundheitsminister:in mit der Vollziehung des Medizinische Assistenzberufe-Gesetzes betraut ist.
- § 88 des Medizinischer Masseur- und Heilmasseurgesetzes in Verbindung mit Teil 2 lit. L Z 11 der Anlage zu § 2 des Bundesministeriengesetzes 1986, wonach die Gesundheitsminister:in mit der Vollziehung des Medizinischer Masseur- und Heilmasseurgesetzes betraut ist.
- § 67 Abs. 1 des Bundesgesetzes über die Regelung des medizinisch-technischen Fachdienstes und der Sanitätshilfsdienste in Verbindung mit Teil 2 lit. L Z 11 der Anlage zu § 2 des Bundesministeriengesetzes 1986, wonach die Gesundheitsminister:in mit der Vollziehung des Bundesgesetzes über die Regelung des medizinisch-technischen Fachdienstes und der Sanitätshilfsdienste betraut ist.
- § 93 Abs. 1 des Medizinproduktegesetzes 2021, wonach – grundsätzlich – die Gesundheitsminister:in mit der Vollziehung des Medizinproduktegesetzes 2021 betraut ist.
- § 35 Z 2 des MTD-Gesetzes, wonach – grundsätzlich – die Gesundheitsminister:in mit der Vollziehung des MTD-Gesetzes betraut ist.

- § 38 des Musiktherapiegesetzes, wonach die Gesundheitsminister:in mit der Vollziehung des Musiktherapiegesetzes betraut ist.
- § 9 des Neue-Psychoaktive-Substanzen-Gesetzes, wonach – grundsätzlich – die Gesundheitsminister:in mit der Vollziehung des Neue-Psychoaktive-Substanzen-Gesetzes betraut ist.
- § 20 des Organtransplantationsgesetzes, wonach die Gesundheitsminister:in mit der Vollziehung des Organtransplantationsgesetzes betraut ist.
- § 9 des OSR-Gesetzes, wonach die Gesundheitsminister:in mit der Vollziehung des OSR-Gesetzes betraut ist.
- § 19 des Patientenverfügungs-Gesetzes, wonach die Gesundheitsminister:in im Einvernehmen mit der Justizminister:in mit der Vollziehung des Patientenverfügungs-Gesetzes betraut ist.
- § 16 Abs. 1 des Primärversorgungsgesetzes, wonach die Gesundheitsminister:in mit der Vollziehung des Primärversorgungsgesetzes betraut ist.
- § 17 des Privatkrankenanstalten-Finanzierungsfondsgesetzes, wonach die Gesundheitsminister:in mit der Aufsicht über den Privatkrankenanstalten-Finanzierungsfonds (PRIKRAF) betraut ist.
- § 50 des Psychologengesetzes 2013, wonach – grundsätzlich – die Gesundheitsminister:in mit der Vollziehung des Psychologengesetzes 2013 betraut ist.
- § 17 in Verbindung mit Teil 2 lit. L Z 11 der Anlage zu § 2 des Bundesministeriengesetzes 1986, wonach – grundsätzlich – die Gesundheitsminister:in mit der Vollziehung des Psychotherapiegesetzes betraut ist.
- § 17 in Verbindung mit Teil 2 lit. L Z 11 der Anlage zu § 2 des Bundesministeriengesetzes 1986, wonach die Gesundheitsminister:in mit der Vollziehung des Reichssanitätsgesetzes betraut ist.
- § 9 des Rezeptpflichtgesetzes, wonach – grundsätzlich – die Sozialminister:in mit der Vollziehung des Rezeptpflichtgesetzes betraut ist.
- § 17 in Verbindung mit Teil 2 lit. L Z 9 („übertragbare Krankheiten“) der Anlage zu § 2 des Bundesministeriengesetzes 1986, wonach die Gesundheitsminister:in mit der Vollziehung des Bundesgesetzes betreffend die sanitäre Regelung des Ammenwesens betraut ist.
- § 17 in Verbindung mit Teil 2 lit. L Z 11 der Anlage zu § 2 des Bundesministeriengesetzes 1986, wonach die Gesundheitsminister:in mit der Vollziehung des Sanitätsgesetzes betraut ist.
- § 15 des Sterbeverfügungsgesetzes, wonach die Gesundheitsminister:in mit der Vollziehung des Sterbeverfügungsgesetzes betraut ist.
- § 155 Abs. 1 Z 1 des Strahlenschutzgesetzes 2020, wonach – zumindest teilweise – die Gesundheitsminister:in mit der Vollziehung des Strahlenschutzgesetzes 2020 betraut ist.
- § 50 Abs. 1 des Suchtmittelgesetzes, wonach – zumindest teilweise – die Gesundheitsminister:in mit der Vollziehung des Suchtmittelgesetzes betraut ist.
- § 19 des Tabak- und Nichtraucherinnen- bzw. Nichtraucherschutzgesetzes, wonach – grundsätzlich – die Gesundheitsminister:in mit der Vollziehung des Tabak- und Nichtraucherinnen- bzw. Nichtraucherschutzgesetzes betraut ist.
- § 56 des Tuberkulosegesetzes, wonach – grundsätzlich – die Gesundheitsminister:in mit der Vollziehung des Tuberkulosegesetzes betraut ist.
- § 17 in Verbindung mit Teil 2 lit. L Z 11 der Anlage zu § 2 des Bundesministeriengesetzes 1986, wonach die Gesundheitsminister:in mit der Vollziehung des Gesetzes über die Vereinheitlichung des Gesundheitswesens betraut ist.
- § 91 des Zahnärztegesetzes, wonach – grundsätzlich – die Gesundheitsminister:in mit der Vollziehung des Zahnärztegesetzes betraut ist.
- § 127 des Zahnärztekammergesetzes, wonach – grundsätzlich – die Gesundheitsminister:in mit der Vollziehung des Zahnärztekammergesetzes betraut ist.

- § 17 in Verbindung mit Teil 2 lit. L Z 9 („übertragbare Krankheiten“) der Anlage zu § 2 des Bundesministerengesetzes 1986, wonach die Gesundheitsminister:in mit der Vollziehung des Zoonosengesetzes betraut ist.

Auch wenn die Steuerung nicht auf Gesetze beschränkt ist, mit deren Vollziehung ausschließlich die Gesundheitsminister:in betraut ist, stellen derartige Gesetze den Schwerpunkt der Steuerungsbestimmungen dar. Auch benachbarte Rechtsgebiete, wie insbesondere das Sozialversicherungsrecht, können wesentliche Auswirkungen auf eine „*qualitativ hochwertige, ausgewogene und allgemein zugängliche medizinische Versorgung*“ (VfGH 30.06.2022, G 334/2021) haben. Aus diesem Grund verweist die Definition der Primärdaten auch auf den „Gesundheits- und Sozialbereich (Art. 9 Abs. 2 Buchstabe h DSGVO)“. Die Grenze ist anhand der Zweckbestimmung in § 11 Abs. 2 des Gesundheits-Zielsteuerungsgesetzes zu ziehen. Während Änderungen von Bauvorschriften zwar geringfügige, aber ebene keine wesentlichen Auswirkungen auf die Struktur, Organisation, Qualität und Finanzierung der österreichischen Gesundheitsversorgung haben können, ist das bei sozialversicherungsrechtlichen Bestimmungen anders: Änderungen im Sozialversicherungsrecht können durchaus wesentliche Auswirkungen auf die Struktur, Organisation, Qualität und Finanzierung der österreichischen Gesundheitsversorgung haben.

Die Erläuterungen zu Art. 51 Abs. 9 B-VG (ErläutRV 203 BlgNR 23. GP 9) führen zur wirkungsorientierten Verwaltung Folgendes aus: *„Bei den Maßnahmen für eine wirkungsorientierte Verwaltung wird es darauf ankommen, die Verknüpfung von Ergebnis- und Ressourcenverantwortung unter Nutzung internationaler Erfahrungen so vorzunehmen, dass diese in effizienter, unbürokratischer Weise umgesetzt wird. Die zugrunde liegende Absicht muss stets handlungsleitend bleiben, nämlich die Steuerung der eingesetzten Mittel nach beabsichtigten Wirkungen und Leistungen mit einem vertretbaren Verwaltungsaufwand vorzunehmen und Verantwortlichen in Politik und Verwaltung aussagekräftige und ohne unzumutbaren Aufwand verarbeitbare Informationen zur Hand zu geben, die diese Verantwortlichen für ihre Steuerungsaufgaben benötigen und die gleichzeitig einer breiten, interessierten Öffentlichkeit deutlich machen, welche Zusammenhänge zwischen eingesetzten Mitteln und Wirkungen/Leistungen bestehen.“* Die verfassungsrechtlich vorgesehene wirkungsorientierte Verwaltung setzt also die Steuerung nach beabsichtigten Wirkungen und Leistungen voraus. Welche Wirkungen und Leistungen beabsichtigt sind, ist den jeweiligen Materien Gesetzen zu entnehmen.

Die Steuerung zur Erreichung dieser Wirkung ist somit nicht nur zulässig, sondern vielmehr – aufgrund der (in völlig herrschender Judikatur) vorgesehenen verfassungskonformen Interpretation (vgl. u.a. VfSlg. 15.199/1998; 6610/1971; 5923/1969; 3297/1957) – sogar geboten.

Da **die angestrebten Ergebnisse nicht vorhanden** sind, bedarf es einer aussagekräftigen Datenevidenz als Voraussetzung für funktionierende, nachvollziehbare und somit transparente einheitliche Steuerungsprozesse (periodisches Planungs- und Berichtswesen) und einheitliche Steuerungsinstrumente, um diese Steuerungsaufgabe erfüllen zu können.

Dass **konkrete Finanzierungs- bzw. Unterstützungszusagen von mehr als drei mit dem Thema befassten staatlichen Einrichtungen**, nämlich von Bund, Ländern und Sozialversicherung vorliegen, ist durch Art. 14 Abs. 1 und Art. 52 Abs. 1 Z 1 lit. e der Art 15a-Vereinbarung über die Organisation und Finanzierung des Gesundheitswesens evident.

Somit besteht sogar ein erhebliches öffentliches Interesse, das gemäß Art. 9 Abs. 2 DSGVO sogar zur Verarbeitung sensibler Daten ermächtigt. Dies deckt sich mit der Ansicht des Verfassungsgerichtshofes, der bereits im Jahr 2006

festgehalten hat, dass ein „[w]ichtiges öffentliches Interesse an einer möglichst kostengünstigen Steuerung des Gesundheitswesens“ besteht (VfSlg. 17.869/2006). Dass sich diese Ansicht nicht geändert hat, bestätigt der VfGH u.a. im Juni 2022, indem er ausdrücklich anerkennt, „dass eine geordnete Krankenanstaltenplanung der Aufrechterhaltung einer qualitativ hochwertigen, ausgewogenen und allgemein zugänglichen medizinischen Versorgung und der Vermeidung einer erheblichen Gefährdung des finanziellen Gleichgewichts des Systems der sozialen Sicherheit und damit dem wichtigen öffentlichen Interesse an einem funktionierenden Gesundheitswesen dient“ (VfGH 30.06.2022, G 334/2021).

Darüber hinaus darf hinsichtlich dieses erheblichen öffentlichen Interesses auf die Ausführungen oben zu Feld „BEWERTUNG / Legitimer Zweck“ verwiesen werden.

Zur Rechtmäßigkeit der Verarbeitung ist auch erforderlich, dass die Anforderungen an die **Determinierung** eingehalten werden. Da die Bestimmungen des Art. 9 Abs. 2 Buchstabe g, h und i DSGVO durch Verweis auf das „Recht eines Mitgliedstaats“ keine Vorgabe zur Rechtsform, insbesondere, ob eine Regelung auf Gesetzes- oder Verordnungsebene zu erfolgen hat, machen, ist hinsichtlich der Determinierung die nationale (VfGH-)Judikatur einschlägig. Diese erlaubt – trotz eines formellen Gesetzesvorbehaltes in § 1 DSG – sowohl unbestimmte Gesetzesbegriffe (VfSlg. 20.446/2021; 19.738/2013) als auch ein Ermessen der Behörde (VfSlg. 19.738/2013) als auch die nähere Determinierung durch Verordnung (VfSlg. 18.146/2007). Hingegen sind Eingriffsermächtigungen, die wie folgt bloß auf die Notwendigkeit für die Vollziehung abstellen („sind verpflichtet [...] die Auskünfte zu erteilen, die für den Vollzug dieses Gesetzes und der relevanten internationalen Vorschriften notwendig sind“), nicht ausreichend determiniert (VfSlg. 16.369/2001). Zu dieser Entscheidung ist anzumerken, dass die wesentlich aktuellere Entscheidung zu § 1 des Auskunftspflichtgesetzes (VfSlg. 20.446/2021) eine vergleichbare Bestimmung erst kürzlich als zulässig anerkannt hat. Außerdem ist die zu § 11 G-ZG vorgeschlagene Bestimmung wesentlich strenger determiniert als die der Entscheidung VfSlg. 16.369/2001 zugrundeliegende Bestimmung. Dieses Mehr an Determinierung ergibt sich insbesondere aus:

- § 3 Z 9 G-ZG, womit die Primärdaten näher definiert werden;
- § 11 Abs. 1 G-ZG, womit die Art der Verarbeitung näher definiert wird;
- § 11 Abs. 2 G-ZG, womit der Zweck der Verarbeitung näher definiert wird;
- § 11 Abs. 3 G-ZG, womit die Datenbereitstellungspflicht der Gesundheits-Zielsteuerungspartner näher definiert wird;
- § 11 Abs. 4 G-ZG, womit technische und organisatorische Maßnahmen zum Schutz der verarbeiteten Daten festgelegt werden;
- § 11 Abs. 5, 6 und 8 G-ZG, womit ein Gremium zur Steuerung der Datenauswertepattform sowie die Aufgaben und Arbeitsweise dieses Gremiums festgelegt werden;
- § 11 Abs. 7 G-ZG, womit eine Verordnungsermächtigung zur näheren Determinierung der Datenbereitstellungspflicht vorgesehen wird.

Die Regelungen sind damit hinsichtlich des Determinierungsgrades nicht mit dem Halbsatz vergleichbar, der in VfSlg. 16.369/2001 zur Aufhebung der betreffenden Bestimmung geführt hat. Auch die Entscheidung des EuGH 20.5.2003, C-465/00 „ORF u.a.“ bzw. VfSlg. 17.065/2003 steht der Bestimmung des § 11 G-ZG nicht entgegen, weil damals die sparsame und effiziente Verwendung öffentlicher Mittel auch durch einen gelinderen Eingriff als die Veröffentlichung der Bezüge unter Namensnennung möglich gewesen wäre. Damit unterscheidet sich der damalige Anlassfall vom Regelungsmotiv des § 11 G-ZG: die oben angeführten Betriebs- und Vollziehungskennzahlen stehen schlichtweg nicht zur Verfügung und können auch nicht durch gelindere Mittel als eine indirekt personenbezogene Verarbeitung erstellt werden.

	<p>Dass die Regelung ein gewisses Abstraktionsniveau aufweist, steht der Rechtmäßigkeit – wie bereits oben ausgeführt – nicht entgegen. Auch der EGMR hat in der Entscheidung „GRA Stiftung gegen Rassismus und Antisemitismus / Schweiz“ einen hohen Abstraktionsgrad anerkannt und festgestellt, dass bei Eingriffen in das Grundrecht auf freie Meinungsäußerung (Art. 10 EMRK) Anforderungen an die Determinierung einzuhalten sind, damit die Eingriffe für die Normadressatinnen und -adressaten vorhersehbar sind, sodass sie ihr Verhalten danach ausrichten können, weil sie die Folgen ihres Verhalten mit einem entsprechenden Grad an Gewissheit erkennen können. Diese Folgen müssen allerdings nicht mit absoluter Sicherheit voraussehbar sein: Die Erfahrung zeigt, dass dies unerreichbar ist. Obwohl diese Sicherheit äußerst erstrebenswert wäre, könnte sie eine übertriebene Starrheit zur Folge haben, das Recht muss jedoch die Möglichkeit haben, mit sich ändernden Gegebenheiten Schritt zu halten. Folglich sind viele Gesetze zwangsläufig so formuliert, dass sie mehr oder weniger unbestimmt und ihre Interpretation und Anwendung eine Frage der Praxis sind (EGMR 09.01.2018, 18597/13 „GRA Stiftung gegen Rassismus und Antisemitismus / Schweiz“ Rn 45 ff). Wenn die genaue Vorhersehbarkeit mit absoluter Sicherheit im Kontext von Art. 10 EMRK unerreichbar ist, wird sie das auch im Kontext von Art. 8 EMRK, d.h. dem Schutzbereich der Datenschutz-Grundverordnung, sein (vgl. auch: EGMR 17.05.2018, 19017/16 „Ljatifi / Mazedonien“ Rn 35).</p> <p>Vor dem Hintergrund der oben zitierten VfGH-Judikatur (VfSlg. 20.446/2021; 19.738/2013; VfSlg. 18.146/2007) sowie der Judikatur der Datenschutzbehörde zum Bundesministerengesetz 1986 stellt § 11 G-ZG die Eingriffsermächtigung dar, die es braucht, um diese Datenflüsse in Übereinstimmung mit dem Grundrecht auf Datenschutz korrekt abzubilden. Die einschlägige Judikatur der Datenschutzbehörde bzw. ihrer Vorgängerbehörde zum Bundesministerengesetz 1986 stellt sich zusammengefasst wie folgt dar:</p> <ul style="list-style-type: none"> ▪ Bestimmungen des Bundesministerengesetzes 1986 alleine stellen keine eigenständige Eingriffsermächtigung dar (DSB 12.04.2019, DSB-D123.591/0003-DSB/2019). ▪ Bestimmungen des Bundesministerengesetzes 1986 in Verbindung mit anderen (allgemeinen) Eingriffsermächtigungen – wie etwa dem ehemaligen § 47 DSG 2000 – hingegen schon (DSK 16.12.2011, K121.739/0013-DSK/2011). <p>Die Anforderung “Bewertung der Rechtmäßigkeit der Verarbeitung” ist somit, insbesondere aufgrund des in Art. 20 Abs. 1 und Art. 77 B-VG grundgelegten Organisationskonzepts der Bundesverfassung, der in Art. 76 B-VG vorgesehenen parlamentarischen Kontrolle sowie im Lichte der einschlägigen Judikatur des EGMR, VfGH und der Datenschutzbehörde, als erfüllt anzusehen.</p>
<p>Angemessenheit der Verarbeitung <small>(Art. 35 Abs. 7 Buchstabe b iVm Art. 5 Abs. 1 Buchstabe c DSGVO; WP 248 Rev.01, 21 und 28)</small></p>	<p>Die Verarbeitung ist vor allem deswegen angemessen, weil mit dem bPK-System eine Pseudonymisierung zwingend vorgeschrieben wird (§ 11 Abs. 4 Z 2 G-ZG). Außerdem dürfen die Betriebs- und Vollziehungskennzahlen (siehe oben Feld „BESCHREIBUNG / Personenbezogene Daten“) nur verarbeitet werden, wenn es eine entsprechende zugrundeliegende gesetzliche Verpflichtung gibt, die für Zwecke gemäß § 11 Abs. 2 G-ZG „in Zahlen gegossen werden muss“. Auch ist geplant eine interne Datenschutz-Richtlinie zu erlassen, die eine interne Beschränkung der Zugriffe vorsieht.</p> <p>Außerdem ist die Verarbeitung angemessen, weil Datenschutz zur Vermeidung der „<i>Erschwerung der Verwaltungsführung</i>“ eingeschränkt werden darf (VfSlg. 17.940/2006) und insbesondere die Verarbeitung durch Beamt:innen (im strafrechtlichen Sinne) aufgrund der strengen rechtlichen Vorgaben für Beamt:innen, eine angemessene organisatorische Maßnahme im Sinne des Art. 32 DSGVO darstellt. Die Einschränkung des Datenschutz ergibt sich aus der Verarbeitungstätigkeit selbst; ebenso die Vermeidung der Erschwerung der Verwaltungsführung, indem mit der vorgeschlagenen Datenauswertepattform erstmals eine elektronisch optimierte</p>

	<p>Evidenzbasierung und Evaluierung möglich sein wird, um beispielsweise die Zahl der verfügbaren Betten einzelfallbezogen, möglichst genau und auf Knopfdruck feststellen zu können (<i>Rechnungshof</i>, Gesundheitsdaten zur Pandemiebewältigung im ersten Jahr der COVID-19-Pandemie, Reihe BUND 2021/43, TZ 19.2). In der Pandemie waren die Daten nämlich erst mit rund achtwöchiger Verspätung verfügbar (<i>Rechnungshof</i>, Gesundheitsdaten zur Pandemiebewältigung im ersten Jahr der COVID-19-Pandemie, Reihe BUND 2021/43, TZ 19.2).</p> <p>Die Anforderung “Bewertung der Angemessenheit der Verarbeitung” ist insbesondere aufgrund des gesetzlich verpflichtenden Einsatzes von bereichsspezifischen Personenkennzeichen, der inhaltlichen Beschränkung auf das Monitoring gesetzlicher Pflichten sowie des strafrechtlichen Schutzes vor Missbrauch, als erfüllt anzusehen.</p>
<p>Erheblichkeit der Verarbeitung <small>(Art. 35 Abs. 7 Buchstabe b iVm Art. 5 Abs. 1 Buchstabe c DSGVO; WP 248 Rev.01, 21 und 28)</small></p>	<p>Die Verantwortlichkeit der obersten Organe stellt einen „<i>Grundgedanken der Verfassung</i>“ dar (VfSlg. 3054/1956). Zu deren Einhaltung müssen die obersten Organe, d.h. u.a. auch die Gesundheitsminister:in effektiv Steuerungs- und Lenkungenfunktionen wahrnehmen; kann sie dies nicht, sind entgegenstehende einfachgesetzliche Bestimmungen verfassungswidrig (VfSlg. 17.421/2004). Dazu bedarf es Informationen. Einfachgesetzliche Bestimmungen, die die „<i>umfassende und rechtzeitige Information des Bundesministers nicht sichern</i>“ (VfSlg. 16.400/2001), beschränken in verfassungswidriger Weise die Leitungs- und Organisationsverantwortung der dem Parlament gegenüber gemäß Art. 76 B-VG verantwortlichen Bundesminister:innen (VfSlg. 16.400/2001). Auch darf das Sachlichkeitsgebot gemäß Art. 7 B-VG nicht übersehen werden: Demnach ist es dem einfachen Gesetzgeber verwehrt, unsachliche Bestimmungen zu erlassen. Aus „<i>gesundheits- und präventionspolitischen Gründen [ist es beispielsweise] erforderlich, ein Mindestmaß an wissenschaftlichen Informationen zu [...] Produkten für die zuständigen Behörden zu erlangen</i>“ (VfSlg. 20.151/2017).</p> <p>Neben einer Verletzung der verfassungsrechtlichen Vorgaben birgt eine nicht (ausreichend) evidenzbasierte Gesundheitspolitik Gefahren für die Gesundheit der in Österreich lebenden Menschen. Im internationalen Vergleich ist in Österreich nicht so sehr die <i>Verfügbarkeit</i> von steuerungsrelevanten Datensets die Herausforderung, sondern deren <i>Verknüpfbarkeit</i> (vgl. <i>OECD</i>, <i>OECD Health Working Paper No. 127</i>, 46, wonach ca 92% Verfügbarkeit aber nur ca 33% Verknüpfbarkeit besteht; näher dazu auch: <i>OECD</i> 14f). Eine rezente Überblicksarbeit zum Thema Datenverknüpfung für evidenzbasierte Gesundheitspolitik zeigt Ansätze für die Umsetzung von Policy-orientierter Datenverknüpfung (<i>Panteli et al</i>, <i>Health and Care Data – Approaches to data linkage for evidence-informed policy</i>). Eine bessere Verknüpfbarkeit bestehender Datensets verbessert die Steuerung, welche wiederum eine bessere Gesundheitsversorgung zu geringeren Kosten ermöglicht.</p> <p>Folgende Beispiele zeigen die Erheblichkeit anhand konkreter Sachverhalte:</p> <ul style="list-style-type: none"> ▪ Die gemeinsame Verarbeitung von <u>Daten betreffend Diagnose, medizinischer Leistung, Medikation (aus e-Rezept, Heilmittelabrechnung oder eMedikation) und Gesundheits-Outcomes (gegebenenfalls Todesursache)</u> ist erforderlich, um Patientenpopulationen (etwa Betroffene von chronischen Krankheiten mit einer bestimmten medikamentösen Therapie) zu identifizieren, die Risikogruppen konstituieren oder deren Entwicklung für die Planung von Versorgungskapazitäten wesentlich ist. Ohne gemeinsame Verarbeitung von Diagnose-, Leistungs-, Medikations- und Todesursachendaten ist eine Identifikation von Patientenpopulationen und Krankheitspfaden oder eine Evaluierung des Leistungsgeschehens und gesundheitspolitischer Maßnahmen nicht in der erforderlichen Qualität möglich. ▪ Die Verarbeitung von <u>Daten betreffend höchstem erreichtem Bildungsabschluss</u> ist erforderlich, um den sozioökonomischen Status von Patient:innen auf eine Weise abschätzen zu können, ohne auf datenschutzrechtlich eingriffsintensivere Alternativen (wie etwa

Einkommensdaten) zurückgreifen zu müssen. Ohne Verarbeitung des Bildungsstatus ist eine zumindest näherungsweise setting-spezifische Gestaltung oder Evaluierung von Public Health-Maßnahmen (Screening-Programmen, etc.) nicht adäquat möglich, was zu mangelhaften oder überschießenden Maßnahmen führt.

- Die Verarbeitung von Daten betreffend Gesundheitsberufe ist erforderlich, um eine bundesweite einheitliche Personal- und Ressourcenplanung zu unterstützen, weil ohne verknüpfbare Gesundheitspersonaldaten etwa ärztliche Ausbildungs- und Karriereverläufe nicht ausreichend modelliert werden, und somit keine exakten Aussagen zum zukünftig erwartbaren ärztlichen Angebot getroffen werden können und folglich beispielsweise Entscheidungen zu notwendigen Ausbildungskapazitäten nicht ausreichend unterstützt werden können.
- Die gemeinsame Verarbeitung von Daten betreffend Diagnose, medizinischer Leistung, Medikation (aus e-Rezept, Heilmittelabrechnung oder eMedikation) und Gesundheits-Outcomes (Krankensätze, Todesursachen) ist erforderlich, um die Auslastung bzw. Belastung des Versorgungssystems zu monitoren und evaluieren zu können, insbesondere bei spezifischen Krankheitsbildern. Ohne die Möglichkeit, Diagnosen, Leistungen, Heilmittelverbrauchs- und Mediationsdaten mit Outcomes in Verbindung zu bringen, kann nur unzureichend auf Bedarfe und Herausforderungen im Gesundheits- und Sozialwesen bzw. der Versorgung reagiert werden (z.B. Belastung des Gesundheitssystems durch Long- bzw. Post-COVID).

Die Verarbeitung ist somit erheblich, weil ohne die Auswertungen der Datenauswertungsplattform die Gesundheitsminister:innen ihre verfassungsrechtliche Verantwortung für das Gesundheitswesen nicht im bestmöglichen Ausmaß wahrnehmen kann und andernfalls schwerere Grundrechtseingriffe, wie auch die Gefährdung der Gesundheit von Menschen, drohen. Dass das Grundrecht auf Datenschutz nicht über anderen Grundrechten steht, ergibt sich bereits aus der Datenschutz-Grundverordnung selbst. So erklärt Erwägungsgrund 4, dass die „*Verarbeitung personenbezogener Daten [...] im Dienste der Menschheit stehen [sollte]*“. Außerdem steht die DSGVO „*im Einklang mit allen Grundrechten*“ und erlaubt u.a. in Art. 9 Abs. 2 Buchstaben c, h und i DSGVO ausdrücklich die Verarbeitung zum Schutz der Gesundheit. Auch eine nationale Rechtsgutanalyse zeigt nachvollziehbar, dass die österreichische Rechtsordnung das Rechtsgut „Gesundheit“ besser schützt als das Rechtsgut „Datenschutz“ und daher – zumindest implizit – als höherwertig ansieht (Reimer/Stanonik, 108). Ähnlich hat der deutsche Sachverständigenrat in seinem Gutachten „Digitalisierung für Gesundheit“ aus dem Jahr 2021 in [Randnummer 712](#) Folgendes dazu festgehalten:

Bei der Pandemiebekämpfung mussten zum Schutze von Leben und Gesundheit vorübergehende Einschränkungen vieler Grundrechte hingenommen werden, gleichzeitig wurde der Datenschutz in seiner einseitigen Ausprägung nicht ernsthaft hinterfragt. Während eine große Zahl von Smartphone-Anwenderinnen und -Anwendern in Deutschland die eigene Ortung und andere weitreichende Datenverwendungen gestattet, um das Komfort-Serviceangebot von Kartendiensten, Browsern und Verkehrsflussanalysen zu nutzen, wurde kein Weg gesucht, Ortungsdaten für die Kontaktverfolgung, Infektionsbekämpfung und den Schutz von Menschenleben und Grundrechten auszuwerten. Man hat stattdessen Ausgangssperren für ganze Bundesländer verhängt. Dabei ließen sich anhand von Ortungsdaten wichtige medizinische und epidemiologische Erkenntnisse zum Infektionsgeschehen gewinnen, die zu differenzierten Schutz- und Hygienemaßnahmen führen könnten. Dies hätte neue Chancen für die Reduzierung von Infektionsfällen, für einen besseren Schutz von Leben und Gesundheit und für einen insgesamt grundrechtesschonenderen Weg der Pandemiebekämpfung eröffnet.

Die Anforderung „Bewertung der Erheblichkeit der Verarbeitung“ ist als erfüllt anzusehen, weil die auf Basis der Verarbeitungstätigkeit

	<p>„Datenauswertungsplattform“ durchgeführten Auswertungen <i>conditio sine qua non</i> für eine verfassungsrechtlich erforderliche Steuerung sind.</p>
<p>Beschränktheit der Verarbeitung auf das notwendige Maß (Art. 35 Abs. 7 Buchstabe b iVm Art. 5 Abs. 1 Buchstabe c DSGVO; WP 248 Rev.01, 21 und 28)</p>	<p>Die Einhaltung des Datenminimierungsgrundsatzes gemäß Art. 5 Abs. 1 Buchstabe c DSGVO ist gegeben, weil</p> <ul style="list-style-type: none"> ▪ Primärdaten nur indirekt (mittels bPK) personenbezogen verarbeitet werden dürfen (§ 11 Abs. 4 Z 3 G-ZG); ▪ Auswertungen nur zur Beurteilung gesetzlicher Pflichten, nicht aber der Erstellung von Persönlichkeitsprofilen oder anderen unerlaubten Zwecken durchgeführt werden dürfen (§ 11 Abs. 4 Z 3 in Verbindung mit § 11 Abs. 2 G-ZG); ▪ die Primärdaten nach Erstellung der Auswertung zu löschen sind (§ 11 Abs. 4 Z 4 G-ZG). <p>Hinsichtlich der Erforderlichkeit der Verarbeitung der umfassten Daten darf oben auf Feld „BEWERTUNG / Erheblichkeit der Verarbeitung“ verwiesen werden.</p> <p>Zusätzlich ist vorgesehen, die Einhaltung des Datenminimierungsgrundsatzes durch entsprechende Strategie-Dokumente, wie etwa einer internen Datenschutz-Richtlinie jederzeit belegen zu können.</p> <p>Die Anforderung „Bewertung der Beschränktheit der Verarbeitung auf das notwendige Maß“ ist als erfüllt anzusehen, insbesondere, weil die Verwendung von bereichsspezifischen Personenkennzeichen anstelle von Namen sowie strenge Zweckbeschränkungen und Löschfristen ausdrücklich in § 11 G-ZG vorgesehen sind.</p>
<p>Speicherbegrenzung (Art. 5 Abs. 1 Buchstabe e DSGVO; WP 248 Rev.01, 21 und 28)</p>	<p>Wie bereits oben im Feld „SYSTEMATISCHE BESCHREIBUNG / Speicherdauer“ ausgeführt, ist die Löschfrist in § 11 Abs. 4 Z 4 G-ZG so angegeben, dass die abgeholten Primärdaten nach der Erstellung der angeforderten Auswertungen zu löschen sind.</p> <p>Durch diese ausdrückliche Löschpflicht ist die Anforderung „Bewertung der Speicherbegrenzung“ als erfüllt anzusehen, weil Maßnahmen zur Begrenzung der Speicherdauer gesetzlich vorgeschrieben sind.</p>
<p>Generelle Information der betroffenen Personen (Art. 12 DSGVO; WP 248 Rev.01, 21 und 28)</p>	<p>Eine Datenschutzerklärung liegt für die gegenständliche Verarbeitung noch nicht vor.</p> <p>Die Anforderungen transparenter Information, Kommunikation und für die Ausübung der Rechte der betroffenen Personen gemäß Art. 12 DSGVO sind durch die Bereitstellung einer Datenschutzerklärung zu erfüllen. Aufgrund des Klarheitsgebots gemäß Art. 12 DSGVO haben sich die Zielsteuerungspartner auf eine gemeinsame Datenschutzerklärung zu einigen, womit auch eine bundesweit einheitliche Formulierung sichergestellt werden kann.</p> <p>Die Anforderung „Bewertung der Information der betroffenen Personen bei Erhebung“ ist aufgrund der grundsätzlichen Machbarkeit einer solchen Information als erfüllbar anzusehen.</p>
<p>Information der betroffenen Personen bei Erhebung (Art. 13 DSGVO; WP 248 Rev.01, 21 und 28)</p>	<p>Eine Datenschutzerklärung liegt für die gegenständliche Verarbeitung noch nicht vor.</p> <p>Zur Einhaltung der klaren und einfachen Sprache – siehe oben: Feld „BEWERTUNG / Generelle Informationen der betroffenen Personen“.</p> <p>Die Anforderung „Bewertung der Information der betroffenen Personen bei Erhebung“ ist aufgrund der grundsätzlichen Machbarkeit einer solchen Information als erfüllbar anzusehen.</p>
<p>Information der betroffenen Personen, wenn die Daten</p>	<p>Siehe oben: Feld „BEWERTUNG / Information der betroffenen Personen bei Erhebung“.</p>

<p>nicht bei ihnen erhoben werden (Art. 14 DSGVO; WP 248 Rev.01, 21 und 28)</p>	<p>Die Anforderung “Bewertung der Information der betroffenen Personen, wenn die Daten nicht bei ihnen erhoben werden” ist aufgrund der grundsätzlichen Machbarkeit einer solchen Information als erfüllbar anzusehen.</p>
<p>Auskunftsrecht der betroffenen Personen und Recht auf Datenübertragbarkeit (Art. 15 und 20 DSGVO; WP 248 Rev.01, 21 und 28)</p>	<p>Das Recht auf Auskunft kann elektronisch oder postalisch gegenüber den Gesundheits-Zielsteuerungspartnern wahrgenommen werden. Diese können eine zentrale Anlaufstelle als so genannten „One-Stop-Shop“ benennen. Hier bedarf es eines Rechtsinstruments gemäß Art. 26 DSGVO zur Aufteilung der Pflichten zwischen den Gesundheits-Zielsteuerungspartnern als gemeinsam Verantwortlichen, das entweder in einem Vertrag oder – wie beim eImpffass – in einer Verordnung bestehen kann. Die näheren Modalitäten zur Ausübung des Rechts auf Auskunft sind in der noch zur Verfügung zu stellenden Datenschutzerklärung zu beschreiben.</p> <p>Das Recht auf Datenübertragbarkeit steht gemäß Art. 20 Abs. 1 Buchstabe a DSGVO nicht zu, weil die Verarbeitung</p> <ul style="list-style-type: none"> ▪ weder aufgrund einer Einwilligung (Art. 6 Abs. 1 Buchstabe a oder Art. 9 Abs. 2 Buchstabe a DSGVO) ▪ noch aufgrund eines Vertrags (Art. 6 Abs. 1 Buchstabe b DSGVO), sondern aufgrund des Rechts eines Mitgliedstaats, nämlich des Gesundheits-Zielsteuergesetzes erfolgt. <p>Die Anforderung “Bewertung des Auskunftsrechts der betroffenen Personen und ihres Rechts auf Datenübertragbarkeit” ist aufgrund der grundsätzlichen Umsetzbarkeit als erfüllbar anzusehen.</p>
<p>Recht auf Berichtigung und Löschung (Art. 16, 17 und 19, WP 248 Rev.01, 21 und 28)</p>	<p>Das Recht auf Berichtigung kann elektronisch oder postalisch gegenüber den Gesundheits-Zielsteuerungspartnern wahrgenommen werden. Diese können eine zentrale Anlaufstelle als so genannten „One-Stop-Shop“ benennen. Hier bedarf es eines Rechtsinstruments gemäß Art. 26 DSGVO zur Aufteilung der Pflichten zwischen den Gesundheits-Zielsteuerungspartnern als gemeinsam Verantwortlichen, das entweder in einem Vertrag oder – wie beim eImpffass – in einer Verordnung bestehen kann. Die näheren Modalitäten zur Ausübung des Rechts auf Berichtigung sind in der noch zur Verfügung zu stellenden Datenschutzerklärung zu beschreiben.</p> <p>Das Recht auf Löschung steht gemäß Art. 17 Abs. 3 Buchstabe b DSGVO nicht zu, weil die Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung, der die Gesundheits-Zielsteuerungspartner als Verantwortliche unterliegen, erforderlich ist. Die <i>rechtlichen Verpflichtungen nach dem Recht eines Mitgliedstaats</i> sind in diesem Fall die verfassungsrechtlichen Bestimmungen zur Ministerverantwortlichkeit, wie insbesondere Art. 76 B-VG, sowie die Bestimmungen des Gesundheits-Zielsteuergesetzes in Verbindung mit den jeweiligen Materiengesetzen.</p> <p>Die Anforderung “Bewertung des Rechts auf Berichtigung und Löschung” ist aufgrund der grundsätzlichen Umsetzbarkeit als erfüllbar anzusehen.</p>
<p>Widerspruchsrecht und Recht auf Einschränkung der Verarbeitung (Art. 18, 19 und 21; WP 248 Rev.01, 21 und 28)</p>	<p>Das Recht auf Einschränkung der Verarbeitung ist gegenüber den Gesundheits-Zielsteuerungspartnern wahrzunehmen. Diese können eine zentrale Anlaufstelle als so genannten „One-Stop-Shop“ benennen. Hier bedarf es eines Rechtsinstruments gemäß Art. 26 DSGVO zur Aufteilung der Pflichten zwischen den Gesundheits-Zielsteuerungspartnern als gemeinsam Verantwortlichen, das entweder in einem Vertrag oder – wie beim eImpffass – in einer Verordnung bestehen kann. Die näheren Modalitäten zur Ausübung des Rechts auf Einschränkung der Verarbeitung sind in der noch zur Verfügung zu stellenden Datenschutzerklärung zu beschreiben.</p> <p>Das Widerspruchsrecht steht nicht zu, weil die Verarbeitung weder aufgrund öffentlicher Interessen (Art. 6 Abs. 1 Buchstabe e DSGVO) noch aufgrund</p>

	<p>berechtigter Interessen (Art. 6 Abs. 1 Buchstabe f DSGVO) noch zu Zwecken der Direktwerbung erfolgt. Die Verarbeitung erfolgt – wie oben in Feld „BESCHREIBUNG / Personenbezogene Daten“ näher ausgeführt – entweder aufgrund einer rechtlichen Verpflichtung (Art. 6 Abs. 1 Buchstabe c DSGVO) oder aufgrund des Rechts eines Mitgliedstaats (Art. 9 Abs. 2 DSGVO). Die Verarbeitung könnte zwar als zu Zwecken der Statistik erfolgend angesehen werden, allerdings besteht auch in diesem Fall kein Widerspruchsrecht, weil dieses selbst in Fällen des Art. 89 DSGVO nicht zusteht, wenn die Verarbeitung zu statistischen Zwecken im öffentlichen Interesse – was hinsichtlich der gegenständlichen Datenauswertungsplattform wohl der Fall wäre – erfolgt.</p> <p>Die Anforderung „Bewertung des Widerspruchsrechts und des Rechts auf Einschränkung der Verarbeitung“ ist aufgrund der grundsätzlichen Umsetzbarkeit als erfüllbar anzusehen.</p>
<p>Verhältnis zu Auftragsverarbeitern (Art. 28 DSGVO; WP 248 Rev.01, 21 und 28)</p>	<p>Da die Datenauswertungsplattform noch zu errichten ist (§ 11 Abs. 1 G-ZG), sind hinsichtlich der genauen Festlegung der Auftragsverarbeiter:innen noch allfällige Ausschreibungen abzuwarten. Dabei sind die Anforderungen des Art. 28 DSGVO einzuhalten. Da es kein „anderes Rechtsinstrument nach dem Unionsrecht oder dem Recht eines Mitgliedstaates“ (Art. 28 Abs. 3 DSGVO), d.h. insbesondere keine Bestimmung im Gesundheits-Zielsteuerungsgesetz oder in einer darauf basierenden Verordnung, gibt, die die Anforderungen des Art. 28 Abs. 3 DSGVO erfüllt, sind Auftragsverarbeitungsvereinbarungen abzuschließen. Dies hat gemäß Art. 28 Abs. 9 DSGVO schriftlich zu erfolgen. Die Verantwortung für den Abschluss der Auftragsverarbeitungsvereinbarungen tragen die Zielsteuerungspartner als Verantwortliche.</p> <p>Die Anforderung „Bewertung des Verhältnisses zu Auftragsverarbeiterinnen und Auftragsverarbeitern“ ist aufgrund der grundsätzlichen Umsetzbarkeit als erfüllbar anzusehen.</p>
<p>Schutzmaßnahmen bei der Übermittlung in Drittländer (Kapitel V DSGVO; WP 248 Rev.01, 21 und 28)</p>	<p>Eine Übermittlung in Drittländer ist nicht vorgesehen. Es sind daher keine spezifischen Schutzmaßnahmen für die Übermittlung in Drittländer vorgesehen.</p> <p>Die Anforderung „Bewertung der Schutzmaßnahmen bei der Übermittlung in Drittländer“ ist aufgrund der nicht vorgesehenen Übermittlung in Drittländer als erfüllt anzusehen.</p>
<p>Vorherige Konsultation (Art. 36 und EG 96 DSGVO; WP 248 Rev.01, 21 und 28)</p>	<p>Die vorherige Konsultation der Datenschutzbehörde ist nicht erforderlich, weil die Verantwortlichen folgende Maßnahmen zur Eindämmung der Risiken treffen:</p> <ul style="list-style-type: none"> ▪ die Verarbeitung ist auf Zwecke gemäß § 11 Abs. 2 G-ZG, d.h. insbesondere Steuerung des Gesundheitswesens beschränkt (siehe unten Feld „Minimierung der Verarbeitung personenbezogener Daten“); ▪ Betriebs- und Vollziehungskennzahlen dürfen nur erhoben werden, wenn es eine entsprechende zugrundeliegende materiengesetzliche Verpflichtung gibt, die für Zwecke gemäß § 11 Abs. 2 G-ZG „in Zahlen gegossen werden muss“ (§ 3 Z 9 iVm § 11 Abs. 2 G-ZG); ▪ alle an der Verarbeitung beteiligten Personen unterliegen einer speziellen Verschwiegenheitspflicht (§ 11 Abs. 4 Z 1 G-ZG); ▪ mit dem bPK-System ist eine Pseudonymisierung zwingend vorgeschrieben (§ 11 Abs. 4 Z 2 G-ZG); ▪ Auswertungen dürfen nur (k-)anonymisiert sein (§ 11 Abs. 4 Z 3 G-ZG); ▪ die Primärdaten sind nach der Erstellung der Auswertungen zu löschen (§ 11 Abs. 4 Z 4 G-ZG); ▪ die einzelnen Verarbeitungsschritte sind zu protokollieren (§ 11 Abs. 4 Z 5 G-ZG); ▪ Dokumentation der Rechtsgrundlagen im Rechtsinformationssystem des Bundes (siehe unten Feld „ABHILFEMASSNAHMEN / Transparenz“);

	<ul style="list-style-type: none"> ▪ Einräumung der Betroffenenrechte im Sinne der DSGVO (siehe unten Feld „ABHILFEMASSNAHMEN / Überwachung der Verarbeitung personenbezogener Daten durch die betroffenen Personen“); ▪ Einhaltung umfangreicher Datensicherheitsmaßnahmen (siehe unten Feld „ABHILFEMASSNAHMEN / Datensicherheitsmaßnahmen“). <p>Die Anforderung “Bewertung der vorherigen Konsultation” ist aufgrund der durchgeführten vorherigen Konsultation als erfüllt anzusehen.</p>
<p>RISIKEN Die Risiken sind nach ihrer Ursache, Art, Besonderheit, Schwere und Eintrittswahrscheinlichkeit zu bewerten (Erwägungsgründe 76, 77, 84 und 90 DSGVO). Als Risiken werden in den Erwägungsgründen 75 und 85 DSGVO unter anderem genannt:</p>	
<p>Physische, materielle oder immaterielle Schäden (EG 90 iVm 85 DSGVO; WP 248 Rev.01, 21 und 28)</p>	<p><u>Ursache:</u> Physische, materielle oder immaterielle Schäden können für die betroffenen Personen durch das Aufdecken von Unregelmäßigkeiten entstehen. Da die betroffenen Personen hinsichtlich ihrer Verfehlungen nicht schutzwürdig sind (siehe insbesondere die §§ 78 f der Strafprozessordnung, die innerhalb des gesetzlichen Aufgabenbereichs sogar eine Anzeigepflicht vorsehen), fehlt es an der Rechtswidrigkeit solcher – allenfalls – durch die Datenauswerteplattform aufgedeckten Schäden.</p> <p><u>Art:</u> Denkbar sind beispielsweise materielle oder immaterielle Schäden, die als Folge aufgedeckten Fehlverhaltens auftreten, wie etwa Verdienstentgang. Physische Schäden sind nicht zu erwarten, weil die Datenauswerteplattform keine unmittelbaren physischen Eingriffe nach sich ziehen.</p> <p><u>Besonderheit:</u> Die Besonderheit des gegenständlichen Risikos für physische, materielle oder immaterielle Schäden ergibt sich aus der (theoretischen) Nachverfolgbarkeit der Arbeit von betroffenen Personen.</p> <p><u>Schwere:</u> Bei Verdacht auf gerichtlich strafbares Verhalten der betroffenen Personen im Zuständigkeitsbereich der Gesundheits-Zielsteuerungspartner, sind diese gemäß § 78 der Strafprozessordnung zur Anzeige an die Kriminalpolizei oder Staatsanwaltschaft verpflichtet. Damit sind theoretisch schwere Konsequenzen für die betroffenen Personen verbunden, die allerdings durch die Bestimmungen der Strafprozessordnung gedeckt sind.</p> <p><u>Eintrittswahrscheinlichkeit:</u> Es ist nicht zu erwarten, dass es zu darüber hinausgehenden Schäden für die betroffenen Personen kommt, weil es strenge Vorkehrungen gibt, die vor einer fehlerhaften bzw. missbräuchlichen Verarbeitung schützen sollen, wie etwa:</p> <ul style="list-style-type: none"> ▪ die Verschwiegenheitspflicht für alle an der Verarbeitung beteiligten Personen (§ 11 Abs. 4 Z 1 G-ZG); ▪ die ausschließliche Verarbeitung unter Verwendung bereichsspezifischer Personenkennzeichen (§ 11 Abs. 4 Z 2 G-ZG); ▪ die Beschränkung der Empfänger von Primärdaten auf Gesundheits-Zielsteuerungspartner (§ 11 Abs. 4 Z 3 G-ZG); ▪ die Pflicht zur Löschung der Primärdaten nach Erstellung der Auswertungen (§ 11 Abs. 4 Z 4 G-ZG); ▪ die Protokollierung der einzelnen Verarbeitungsschritte (§ 11 Abs. 4 Z 5 G-ZG); ▪ das für Beamten:innen bei den Gesundheits-Zielsteuerungspartnern geltende Disziplinarrecht; ▪ die für SV-Bedienstete einschlägige SV-Datenschutzverordnung; ▪ Art. 25 DSGVO, der zum Schutz der betroffenen Personen verlangt, dass „geeignete technische und organisatorische Maßnahmen“ zu treffen sind; ▪ Art. 32 DSGVO, wonach Verantwortliche und Auftragsverarbeiter:innen für „ein dem Risiko angemessenes Schutzniveau“ zu sorgen haben;

	<ul style="list-style-type: none"> ▪ strafrechtliche Bestimmungen, wie etwa die Straftatbestände „Verletzung von Berufsgeheimnissen“ (§ 121 StGB), „Amtsmissbrauch“ (§ 302 StGB) oder „Verletzung eines Amtsgeheimnisses“ (§ 310 StGB). <p>Aufgrund der gegenständlichen Verarbeitung, insbesondere der geltenden, strengen Strafdrohungen ist nicht von einem substantziellen Risiko für das Auftreten physischer, materieller und immaterieller Schäden auszugehen, womit die gegenständliche Anforderung als erfüllt angesehen werden kann.</p>
<p>Verlust der Kontrolle über personenbezogene Daten (EG 90 iVm 85 DSGVO; WP 248 Rev.01, 21 und 28)</p>	<p><u>Ursache:</u> Der Verlust der Kontrolle über personenbezogene Daten kann für die betroffenen Personen grundsätzlich durch jede Verarbeitung entstehen und ist bei gesetzlich vorgesehenen Verarbeitungen höher als bei Verarbeitungen aufgrund von Einwilligungen, weil bei gesetzlich vorgesehenen Verarbeitungen die Mitwirkung der betroffenen Personen oftmals nicht erforderlich bzw. vorgesehen ist.</p> <p><u>Art:</u> Beim Verlust der Kontrolle über personenbezogene Daten haben die betroffenen Personen keinerlei Möglichkeit auf die Verarbeitung Einfluss zu nehmen und sind ihrer Betroffenenrechte beraubt.</p> <p><u>Besonderheit:</u> Die Besonderheit des gegenständlichen Risikos für den Verlust der Kontrolle über personenbezogene Daten ergibt sich vor allem aus dem Umfang der verarbeiteten Daten. Dass die gesetzliche vorgesehene Verarbeitung aber nicht unzulässig ist, zeigen die zahlreichen Steuerungsbestimmungen (siehe oben Feld „BEWERTUNG / Rechtmäßigkeit der Verarbeitung“) sowie die Öffnungsklauseln in der Datenschutz-Grundverordnung, die die Verarbeitung aufgrund nationaler Bestimmungen erlauben.</p> <p><u>Schwere:</u> Von ihrer Schwere ist der Verlust der Kontrolle über personenbezogene Daten nicht von vergleichbaren Risiken aufgrund anderer gesetzlich vorgesehener Verarbeitungen zu unterscheiden.</p> <p><u>Eintrittswahrscheinlichkeit:</u> Es ist nicht zu erwarten, dass es zum Verlust der Kontrolle über personenbezogene für die betroffenen Personen kommt, weil es zahlreiche Vorkehrungen gibt, die die Transparenz der Verarbeitung, die Betroffenenrechte sowie den (datenschutzrechtlichen) Rechtsschutz der betroffenen Personen sicherstellen, wie etwa:</p> <ul style="list-style-type: none"> ▪ die Veröffentlichung von § 11 G-ZG, der darauf basierenden Verordnungen gemäß § 11 Abs. 7 G-ZG sowie der materiengesetzlichen Verpflichtungen in Sinne des § 11 G-ZG im Rahmen des Rechtsinformationssystems des Bundes im Internet; ▪ die Möglichkeit zur Geltendmachung ihrer Betroffenenrechte gegenüber allen Verantwortlichen gemäß Art. 26 DSGVO; ▪ die Verschwiegenheitspflicht für alle an der Verarbeitung beteiligten Personen (§ 11 Abs. 4 Z 1 G-ZG); ▪ die ausschließliche Verarbeitung unter Verwendung bereichsspezifischer Personenkennzeichen (§ 11 Abs. 4 Z 2 G-ZG); ▪ die Beschränkung der Empfänger von Primärdaten auf Gesundheits-Zielsteuerungspartner (§ 11 Abs. 4 Z 3 G-ZG); ▪ die Pflicht zur Löschung der Primärdaten nach Erstellung der Auswertungen (§ 11 Abs. 4 Z 4 G-ZG); ▪ die Protokollierung der einzelnen Verarbeitungsschritte (§ 11 Abs. 4 Z 5 G-ZG); ▪ das für Beamten:innen bei den Gesundheits-Zielsteuerungspartnern geltende Disziplinarrecht; ▪ die für SV-Bedienstete einschlägige SV-Datenschutzverordnung; ▪ Art. 25 DSGVO, der zum Schutz der betroffenen Personen verlangt, dass „geeignete technische und organisatorische Maßnahmen“ zu treffen sind; ▪ Art. 32 DSGVO, wonach Verantwortliche und Auftragsverarbeiter:innen für „ein dem Risiko angemessenes Schutzniveau“ zu sorgen haben;

	<ul style="list-style-type: none"> ▪ strafrechtliche Bestimmungen, wie etwa die Straftatbestände „Verletzung von Berufsgeheimnissen“ (§ 121 StGB), „Amtsmissbrauch“ (§ 302 StGB) oder „Verletzung eines Amtsgeheimnisses“ (§ 310 StGB). <p>Aufgrund der gegenständlichen Verarbeitung, insbesondere der geltenden, strengen Strafdrohungen ist nicht von einem substanziellen Risiko für den Verlust der Kontrolle über personenbezogene Daten auszugehen, womit die gegenständliche Anforderung als erfüllt angesehen werden kann.</p>
<p>Diskriminierung (EG 90 iVm 85 DSGVO; WP 248 Rev.01, 21 und 28)</p>	<p><u>Ursache:</u> Nachteile aus Diskriminierung können für die betroffenen Personen grundsätzlich durch jede Verarbeitung personenbezogener Daten entstehen, weil die Verarbeitung personenbezogener Daten die Filterung nach gewissen Merkmalen erlauben und für die so durch Filterung ermittelten betroffenen Personen (rechtswidrigerweise) negative Konsequenzen vorgesehen werden können.</p> <p><u>Art:</u> Denkbar sind Nachteile aus Diskriminierung durch das Bekanntwerden von Verfehlungen der betroffenen Personen. Denkbar wären zudem fehlerhafte Meldungen von Verfehlungen aufgrund von Fehlern in der Programmlogik.</p> <p><u>Besonderheit:</u> Die Besonderheit des gegenständlichen Risikos für Nachteile aus Diskriminierung ergibt sich aus einem allfälligen Vertragsverhältnis der betroffenen Personen zu Sozialversicherungsträgern. Der Dachverband der Sozialversicherungsträger ist nämlich einer der Gesundheits-Zielsteuerungspartner (§ 11 Abs. 1 Z 3 G-ZG).</p> <p><u>Schwere:</u> Diskriminierungen sind theoretisch denkbar; rechtlich vorgesehene Sanktionen sind allerdings nicht als rechtlich verwerfliche Diskriminierungen anzusehen.</p> <p><u>Eintrittswahrscheinlichkeit:</u> Auch wenn durch die Doppelfunktion des Dachverbands der Sozialversicherungsträger – einerseits als Gesundheits-Zielsteuerungspartner und andererseits als Dachverband der Sozialversicherungsträger, dh. potentieller Vertragspartner der betroffenen Personen – eine Diskriminierung theoretisch denkbar ist, fehlt dem rechtlich gedeckten Vorsehen von Sanktionen seitens der Sozialversicherungsträger im Falle von Verfehlungen der betroffenen Personen der (rechtlich verwerfliche) Diskriminierungscharakter. Es ist nicht zu erwarten, dass es zu Nachteilen aus Diskriminierung für die betroffenen Personen kommt, weil es zahlreiche Vorkehrungen gibt, die die Richtigkeit der Verarbeitung sicherstellen, wie etwa:</p> <ul style="list-style-type: none"> ▪ die Verschwiegenheitspflicht für alle an der Verarbeitung beteiligten Personen (§ 11 Abs. 4 Z 1 G-ZG); ▪ die ausschließliche Verarbeitung unter Verwendung bereichsspezifischer Personenkennzeichen (§ 11 Abs. 4 Z 2 G-ZG); ▪ die Beschränkung der Empfänger von Primärdaten auf Gesundheits-Zielsteuerungspartner (§ 11 Abs. 4 Z 3 G-ZG); ▪ die Pflicht zur Löschung der Primärdaten nach Erstellung der Auswertungen (§ 11 Abs. 4 Z 4 G-ZG); ▪ die Protokollierung der einzelnen Verarbeitungsschritte (§ 11 Abs. 4 Z 5 G-ZG); ▪ das für Beamt:innen bei den Gesundheits-Zielsteuerungspartnern geltende Disziplinarrecht; ▪ die für SV-Bedienstete einschlägige SV-Datenschutzverordnung; ▪ Art. 25 DSGVO, der zum Schutz der betroffenen Personen verlangt, dass „geeignete technische und organisatorische Maßnahmen“ zu treffen sind; ▪ Art. 32 DSGVO, wonach Verantwortliche und Auftragsverarbeiter:innen für „ein dem Risiko angemessenes Schutzniveau“ zu sorgen haben;

	<ul style="list-style-type: none"> ▪ strafrechtliche Bestimmungen, wie etwa die Straftatbestände „Verletzung von Berufsgeheimnissen“ (§ 121 StGB), „Amtsmissbrauch“ (§ 302 StGB) oder „Verletzung eines Amtsgeheimnisses“ (§ 310 StGB). <p>Aufgrund der gegenständlichen Verarbeitung, insbesondere der geltenden, strengen Strafdrohungen ist nicht von einem substanziellen Risiko für Diskriminierung der betroffenen Personen auszugehen, womit die gegenständliche Anforderung als erfüllt angesehen werden kann.</p>
<p>Identitätsdiebstahl oder -betrug (EG 90 iVm 85 DSGVO; WP 248 Rev.01, 21 und 28)</p>	<p><u>Ursache:</u> Identitätsdiebstahl oder -betrug treten typischerweise in der Folge von Datenschutzverletzungen (Art. 4 Nr. 12 DSGVO) auf, wenn personenbezogene Daten, wie insbesondere E-Mail-Adressen, Nutzerkennungen, Passwörter oder Kreditkarteninformationen gestohlen oder offengelegt werden.</p> <p><u>Art:</u> Identitätsdiebstahl oder -betrug können zu hohen, finanziellen Schäden bei den betroffenen Personen führen, insbesondere wenn mit den gestohlenen Identitäten kostenpflichtige Services (im Internet) in Anspruch genommen werden. Die betroffenen Personen entdecken den Identitätsdiebstahl oder -betrug oft erst, wenn ihnen nicht bezogene Leistungen in Rechnung gestellt werden.</p> <p><u>Besonderheit:</u> Die Besonderheit des gegenständlichen Risikos für Identitätsdiebstahl oder -betrug ergibt sich vor allem aus der gesetzlichen Regelung, die der Datenauswertepattform zugrunde liegt. Dass weder Passwörter noch Nutzerkennungen oder Kreditkarteninformationen verarbeitet werden, senkt das Risiko für Identitätsdiebstahl oder -betrug.</p> <p><u>Schwere:</u> Identitätsdiebstahl oder -betrug können – wie bereits ausgeführt – zu hohen, finanziellen Schäden bei den betroffenen Personen führen.</p> <p><u>Eintrittswahrscheinlichkeit:</u> Datenschutzverletzungen können nie zur Gänze ausgeschlossen werden. Es ist daher wichtig durch geeignete Prozesse sicherzustellen, dass sie soweit als möglich verhindert werden bzw. im Fall des Falles rasch reagiert wird. Insbesondere sollen typische technische und organisatorische Maßnahmen zur Sicherheit der Datenverarbeitung gemäß Art. 32 DSGVO vorgesehen werden, wie etwa</p> <ul style="list-style-type: none"> ▪ zur zeitlichen Verfügbarkeit, ▪ zu Sicherheitsanforderungen und Zugriffsschutz, ▪ zu Beauftragten für die Informationssicherheit, ▪ zum Risikomanagement, ▪ zu Sicherheitsanforderungen an Prozesse, ▪ zu technische Sicherheitsanforderungen, ▪ zu Sicherheitsanforderungen an die Authentifizierung, ▪ zu Sicherheitsanforderungen für Testumgebungen, ▪ zu baulichen Sicherheitsanforderungen sowie ▪ zu Sicherheitsanforderungen an das Personal. <p>Auch durch die folgenden bereits im Entwurf enthaltenen technischen und organisatorischen Maßnahmen soll die Sicherheit der Verarbeitung erhöht und das Risiko für Identitätsdiebstahl oder -betrug gesenkt werden:</p> <ul style="list-style-type: none"> ▪ die Verschwiegenheitspflicht für alle an der Verarbeitung beteiligten Personen (§ 11 Abs. 4 Z 1 G-ZG); ▪ die ausschließliche Verarbeitung unter Verwendung bereichsspezifischer Personenkennzeichen (§ 11 Abs. 4 Z 2 G-ZG); ▪ die Beschränkung der Empfänger von Primärdaten auf Gesundheits-Zielsteuerungspartner (§ 11 Abs. 4 Z 3 G-ZG); ▪ die Pflicht zur Löschung der Primärdaten nach Erstellung der Auswertungen (§ 11 Abs. 4 Z 4 G-ZG); ▪ die Protokollierung der einzelnen Verarbeitungsschritte (§ 11 Abs. 4 Z 5 G-ZG);

	<ul style="list-style-type: none"> ▪ das für Beamt:innen bei den Gesundheits-Zielsteuerungspartnern geltende Disziplinarrecht; ▪ die für SV-Bedienstete einschlägige SV-Datenschutzverordnung; ▪ Art. 25 DSGVO, der zum Schutz der betroffenen Personen verlangt, dass „geeignete technische und organisatorische Maßnahmen“ zu treffen sind; ▪ Art. 32 DSGVO, wonach Verantwortliche und Auftragsverarbeiter:innen für „ein dem Risiko angemessenes Schutzniveau“ zu sorgen haben; ▪ strafrechtliche Bestimmungen, wie etwa die Straftatbestände „Verletzung von Berufsgeheimnissen“ (§ 121 StGB), „Amtsmissbrauch“ (§ 302 StGB) oder „Verletzung eines Amtsgeheimnisses“ (§ 310 StGB). <p>Aufgrund der gegenständlichen Verarbeitung, insbesondere der geltenden, strengen Strafdrohungen ist nicht von einem substantziellen Risiko für Identitätsdiebstahl oder -betrug auszugehen, womit die gegenständliche Anforderung als erfüllt angesehen werden kann.</p>
<p>Finanzielle Verluste (EG 90 iVm 85 DSGVO; WP 248 Rev.01, 21 und 28)</p>	<p><u>Ursache:</u> Auch finanzielle Verluste treten typischerweise in der Folge von Datenschutzverletzungen (Art. 4 Nr. 12 DSGVO) auf, wenn personenbezogene Daten, wie insbesondere E-Mail-Adressen, Nutzerkennungen, Passwörter oder Kreditkarteninformationen gestohlen oder offengelegt werden. Finanzielle Verluste können sich aber auch als nachteilige Folgen von Diskriminierung ergeben.</p> <p><u>Art:</u> Finanzielle Verluste sind geldwerte Schäden und können insbesondere im Entgang von Verdienstmöglichkeiten liegen.</p> <p><u>Besonderheit:</u> Die Besonderheit des gegenständlichen Risikos für finanzielle Verluste ergibt sich vor allem aus der gesetzlichen Regelung, die der Datenauswertungsplattform zugrunde liegt. Dass weder Passwörter noch Nutzerkennungen noch Kreditkarteninformationen verarbeitet werden, senkt das Risiko für finanzielle Verluste aufgrund von Identitätsdiebstahl oder -betrug.</p> <p><u>Schwere:</u> Identitätsdiebstahl oder -betrug können – wie bereits oben ausgeführt – zu hohen, finanziellen Schäden bei den betroffenen Personen führen.</p> <p><u>Eintrittswahrscheinlichkeit:</u> Es ist nicht zu erwarten, dass es zu finanziellen Verlusten für die betroffenen Personen kommt, weil zahlreiche Vorkehrungen bestehen, die die Rechtmäßigkeit der Verarbeitung sicherstellen sollen, wie etwa:</p> <ul style="list-style-type: none"> ▪ die Verschwiegenheitspflicht für alle an der Verarbeitung beteiligten Personen (§ 11 Abs. 4 Z 1 G-ZG); ▪ die ausschließliche Verarbeitung unter Verwendung bereichsspezifischer Personenkennzeichen (§ 11 Abs. 4 Z 2 G-ZG); ▪ die Beschränkung der Empfänger von Primärdaten auf Gesundheits-Zielsteuerungspartner (§ 11 Abs. 4 Z 3 G-ZG); ▪ die Pflicht zur Löschung der Primärdaten nach Erstellung der Auswertungen (§ 11 Abs. 4 Z 4 G-ZG); ▪ die Protokollierung der einzelnen Verarbeitungsschritte (§ 11 Abs. 4 Z 5 G-ZG); ▪ das für Beamt:innen bei den Gesundheits-Zielsteuerungspartnern geltende Disziplinarrecht; ▪ die für SV-Bedienstete einschlägige SV-Datenschutzverordnung; ▪ Art. 25 DSGVO, der zum Schutz der betroffenen Personen verlangt, dass „geeignete technische und organisatorische Maßnahmen“ zu treffen sind; ▪ Art. 32 DSGVO, wonach Verantwortliche und Auftragsverarbeiter:innen für „ein dem Risiko angemessenes Schutzniveau“ zu sorgen haben; ▪ strafrechtliche Bestimmungen, wie etwa die Straftatbestände „Verletzung von Berufsgeheimnissen“ (§ 121 StGB), „Amtsmissbrauch“ (§ 302 StGB) oder „Verletzung eines Amtsgeheimnisses“ (§ 310 StGB).

	<p>Aufgrund der gegenständlichen Verarbeitung, insbesondere der geltenden, strengen Strafdrohungen ist nicht von finanziellen Verlusten für die betroffenen Personen auszugehen, womit die gegenständliche Anforderung als erfüllt angesehen werden kann.</p>
<p>Unbefugte Aufhebung der Pseudonymisierung (EG 90 iVm 85 DSGVO; WP 248 Rev.01, 21 und 28)</p>	<p><u>Ursache:</u> Die unbefugte Aufhebung der Pseudonymisierung geschieht typischerweise durch Verkettung grundsätzlich pseudonymisierter Datensätze.</p> <p><u>Art:</u> Die unbefugte Aufhebung der Pseudonymisierung kann andere Risiken, wie etwa finanzielle Verluste oder Nachteile aus Diskriminierung zur Folge haben.</p> <p><u>Besonderheit:</u> Die Besonderheit des gegenständlichen Risikos ergibt sich aus der gesetzlichen Regelung, die ausdrücklich eine Pseudonymisierung vorsieht (§ 11 Abs. 4 Z 2 G-ZG).</p> <p><u>Schwere:</u> Die Schwere des Risikos ergibt sich vor allem aus den anschließenden Risiken, wie etwa finanziellen Verlusten oder Nachteilen aus Diskriminierung.</p> <p><u>Eintrittswahrscheinlichkeit:</u> Die Wahrscheinlichkeit für eine unbefugte Aufhebung der Pseudonymisierung ist gering, weil die Verarbeitung wohl ausschließlich von Beamt:innen im strafrechtlichen Sinne durchgeführt wird, die daher strengen gesetzlichen Auflagen, insbesondere des Strafgesetzbuchs unterliegen. Außerdem sind umfangreiche technische und organisatorische Maßnahmen vorgesehen. Zu diesen Maßnahmen zählen etwa:</p> <ul style="list-style-type: none"> ▪ die Verschwiegenheitspflicht für alle an der Verarbeitung beteiligten Personen (§ 11 Abs. 4 Z 1 G-ZG); ▪ die ausschließliche Verarbeitung unter Verwendung bereichsspezifischer Personenkennzeichen (§ 11 Abs. 4 Z 2 G-ZG); ▪ die Beschränkung der Empfänger von Primärdaten auf Gesundheits-Zielsteuerungspartner (§ 11 Abs. 4 Z 3 G-ZG); ▪ die Pflicht zur Löschung der Primärdaten nach Erstellung der Auswertungen (§ 11 Abs. 4 Z 4 G-ZG); ▪ die Protokollierung der einzelnen Verarbeitungsschritte (§ 11 Abs. 4 Z 5 G-ZG); ▪ das für Beamt:innen bei den Gesundheits-Zielsteuerungspartnern geltende Disziplinarrecht; ▪ die für SV-Bedienstete einschlägige SV-Datenschutzverordnung; ▪ Art. 25 DSGVO, der zum Schutz der betroffenen Personen verlangt, dass „geeignete technische und organisatorische Maßnahmen“ zu treffen sind; ▪ Art. 32 DSGVO, wonach Verantwortliche und Auftragsverarbeiter:innen für „ein dem Risiko angemessenes Schutzniveau“ zu sorgen haben; ▪ strafrechtliche Bestimmungen, wie etwa die Straftatbestände „Verletzung von Berufsgeheimnissen“ (§ 121 StGB), „Amtsmissbrauch“ (§ 302 StGB) oder „Verletzung eines Amtsgeheimnisses“ (§ 310 StGB). <p>Aufgrund der gegenständlichen Verarbeitung, insbesondere der geltenden, strengen Strafdrohungen ist nicht von einer unbefugten Aufhebung der Pseudonymisierung – wie sie durch die bereichsspezifischen Personenkennzeichen sichergestellt wird – auszugehen, womit die gegenständliche Anforderung als erfüllt angesehen werden kann.</p>
<p>Rufschädigung (EG 90 iVm 85 DSGVO; WP 248 Rev.01, 21 und 28)</p>	<p><u>Ursache:</u> Nachteile aus Rufschädigung sind theoretisch denkbar.</p> <p><u>Art:</u> Nachteile aus Rufschädigung können sich infolge anderer Risiken, wie etwa Datenschutzverletzungen ergeben.</p> <p><u>Besonderheit:</u> Die Besonderheit des gegenständlichen Risikos für Rufschädigung ergibt sich vor allem aus der großen Zahl an betroffenen Personen, die von dieser gesetzlichen Verarbeitung erfasst sind.</p>

	<p><u>Schwere:</u> Die Schwere des Risikos kann theoretisch – je nach Art der potentiellen Rufschädigung – auch hoch sein.</p> <p><u>Eintrittswahrscheinlichkeit:</u> Nachteile durch Rufschädigung sind eher nicht zu erwarten, weil den typischerweise mit einer Rufschädigung verbundenen Nachteilen durch technische und organisatorische Maßnahmen zur Sicherstellung der Vertraulichkeit und insbesondere Minimierung der Daten begegnet wird. Zu diesen Maßnahmen zählen etwa:</p> <ul style="list-style-type: none"> ▪ die Verschwiegenheitspflicht für alle an der Verarbeitung beteiligten Personen (§ 11 Abs. 4 Z 1 G-ZG); ▪ die ausschließliche Verarbeitung unter Verwendung bereichsspezifischer Personenkennzeichen (§ 11 Abs. 4 Z 2 G-ZG); ▪ die Beschränkung der Empfänger von Primärdaten auf Gesundheits-Zielsteuerungspartner (§ 11 Abs. 4 Z 3 G-ZG); ▪ die Pflicht zur Löschung der Primärdaten nach Erstellung der Auswertungen (§ 11 Abs. 4 Z 4 G-ZG); ▪ die Protokollierung der einzelnen Verarbeitungsschritte (§ 11 Abs. 4 Z 5 G-ZG); ▪ das für Beam:innen bei den Gesundheits-Zielsteuerungspartnern geltende Disziplinarrecht; ▪ die für SV-Bedienstete einschlägige SV-Datenschutzverordnung; ▪ Art. 25 DSGVO, der zum Schutz der betroffenen Personen verlangt, dass „geeignete technische und organisatorische Maßnahmen“ zu treffen sind; ▪ Art. 32 DSGVO, wonach Verantwortliche und Auftragsverarbeiter:innen für „ein dem Risiko angemessenes Schutzniveau“ zu sorgen haben; ▪ strafrechtliche Bestimmungen, wie etwa die Straftatbestände „Verletzung von Berufsgeheimnissen“ (§ 121 StGB), „Amtsmissbrauch“ (§ 302 StGB) oder „Verletzung eines Amtsgeheimnisses“ (§ 310 StGB). <p>Aufgrund der gegenständlichen Verarbeitung, insbesondere der geltenden, strengen Strafdrohungen ist nicht von einer Rufschädigung für betroffene Personen auszugehen, womit die gegenständliche Anforderung als erfüllt angesehen werden kann.</p>
<p>Verlust der Vertraulichkeit bei Berufsgeheimnissen (EG 90 iVm 85 DSGVO; WP 248 Rev.01, 21 und 28)</p>	<p><u>Ursache:</u> Der Verlust der Vertraulichkeit bei Berufsgeheimnissen ist theoretisch denkbar, wenn es zu Offenlegung durch Personen, die etwa dem Amtsgeheimnis unterliegen, kommt.</p> <p><u>Art:</u> Der Verlust der Vertraulichkeit bei Berufsgeheimnissen kann andere Risiken, wie etwa finanzielle Verluste oder Nachteile aus Diskriminierung zur Folge haben.</p> <p><u>Besonderheit:</u> Die Besonderheit des gegenständlichen Risikos ergibt sich vor allem daraus, dass die Verarbeitung nur durch Personen erfolgen darf, die einem Berufsgeheimnis (gemäß § 11 Abs. 4 Z 1 G-ZG) unterliegen.</p> <p><u>Schwere:</u> Die Schwere des Risikos ergibt sich vor allem aus den anschließenden Risiken, wie etwa finanziellen Verlusten oder Nachteilen aus Diskriminierung.</p> <p><u>Eintrittswahrscheinlichkeit:</u> Den typischerweise mit dem Verlust der Vertraulichkeit bei Berufsgeheimnissen verbundenen Nachteilen ist durch technische und organisatorische Maßnahmen zur Sicherstellung der Vertraulichkeit zu begegnen. Zu diesen Maßnahmen zählen etwa:</p> <ul style="list-style-type: none"> ▪ die Verschwiegenheitspflicht für alle an der Verarbeitung beteiligten Personen (§ 11 Abs. 4 Z 1 G-ZG); ▪ die ausschließliche Verarbeitung unter Verwendung bereichsspezifischer Personenkennzeichen (§ 11 Abs. 4 Z 2 G-ZG); ▪ die Beschränkung der Empfänger von Primärdaten auf Gesundheits-Zielsteuerungspartner (§ 11 Abs. 4 Z 3 G-ZG);

	<ul style="list-style-type: none"> ▪ die Pflicht zur Löschung der Primärdaten nach Erstellung der Auswertungen (§ 11 Abs. 4 Z 4 G-ZG); ▪ die Protokollierung der einzelnen Verarbeitungsschritte (§ 11 Abs. 4 Z 5 G-ZG); ▪ das für Beamt:innen bei den Gesundheits-Zielsteuerungspartnern geltende Disziplinarrecht; ▪ die für SV-Bedienstete einschlägige SV-Datenschutzverordnung; ▪ Art. 25 DSGVO, der zum Schutz der betroffenen Personen verlangt, dass „geeignete technische und organisatorische Maßnahmen“ zu treffen sind; ▪ Art. 32 DSGVO, wonach Verantwortliche und Auftragsverarbeiter:innen für „ein dem Risiko angemessenes Schutzniveau“ zu sorgen haben; ▪ strafrechtliche Bestimmungen, wie etwa die Straftatbestände „Verletzung von Berufsgeheimnissen“ (§ 121 StGB), „Amtsmissbrauch“ (§ 302 StGB) oder „Verletzung eines Amtsgeheimnisses“ (§ 310 StGB). <p>Aufgrund der gegenständlichen Verarbeitung, insbesondere der geltenden, strengen Strafdrohungen ist nicht von einem Verlust der Vertraulichkeit bei Berufsgeheimnissen auszugehen, womit die gegenständliche Anforderung als erfüllt angesehen werden kann.</p>
<p>Erhebliche wirtschaftliche oder gesellschaftliche Nachteile (EG 90 iVm 85 DSGVO; WP 248 Rev.01, 21 und 28)</p>	<p><u>Ursache:</u> Erhebliche wirtschaftliche oder gesellschaftliche Nachteile sind für die betroffenen Personen kaum denkbar (siehe oben Feld „RISIKEN / Physische, materielle oder immaterielle Schäden“, Seite 24 bzw. Feld „RISIKEN / Diskriminierung“, Seite 26), insbesondere weil die Möglichkeiten für Identitätsdiebstahl oder -betrug begrenzt sind.</p> <p><u>Art:</u> Theoretisch denkbar sind erhebliche wirtschaftliche oder gesellschaftliche Nachteile durch das Bekanntwerden von Verfehlungen seitens der betroffenen Personen. Denkbar wären zudem fehlerhafte Meldungen von Verfehlungen aufgrund von Fehlern in der Programmlogik.</p> <p><u>Besonderheit:</u> Die Besonderheit des gegenständlichen Risikos für Nachteile aus Diskriminierung ergibt sich aus einem allfälligen Vertragsverhältnis der betroffenen Personen zu Sozialversicherungsträgern. Der Dachverband der Sozialversicherungsträger ist nämlich einer der Gesundheits-Zielsteuerungspartner (§ 11 Abs. 1 Z 3 G-ZG).</p> <p><u>Schwere:</u> Erhebliche wirtschaftliche oder gesellschaftliche Nachteile können vor allem den Verlust von Vertragsverhältnissen zu Sozialversicherungsträgern oder strafrechtliche Konsequenzen umfassen.</p> <p><u>Eintrittswahrscheinlichkeit:</u> Es ist nicht zu erwarten, dass es zu (unzulässigen) erheblichen wirtschaftlichen oder gesellschaftlichen Nachteilen für die betroffenen Personen kommt, weil zahlreiche technische und organisatorische Maßnahmen vorgesehen sind, die die Vertraulichkeit der Verarbeitung sicherstellen sollen, wie etwa:</p> <ul style="list-style-type: none"> ▪ die Verschwiegenheitspflicht für alle an der Verarbeitung beteiligten Personen (§ 11 Abs. 4 Z 1 G-ZG); ▪ die ausschließliche Verarbeitung unter Verwendung bereichsspezifischer Personenkennzeichen (§ 11 Abs. 4 Z 2 G-ZG); ▪ die Beschränkung der Empfänger von Primärdaten auf Gesundheits-Zielsteuerungspartner (§ 11 Abs. 4 Z 3 G-ZG); ▪ die Pflicht zur Löschung der Primärdaten nach Erstellung der Auswertungen (§ 11 Abs. 4 Z 4 G-ZG); ▪ die Protokollierung der einzelnen Verarbeitungsschritte (§ 11 Abs. 4 Z 5 G-ZG); ▪ das für Beamt:innen bei den Gesundheits-Zielsteuerungspartnern geltende Disziplinarrecht; ▪ die für SV-Bedienstete einschlägige SV-Datenschutzverordnung; ▪ Art. 25 DSGVO, der zum Schutz der betroffenen Personen verlangt, dass „geeignete technische und organisatorische Maßnahmen“ zu treffen sind;

	<ul style="list-style-type: none"> ▪ Art. 32 DSGVO, wonach Verantwortliche und Auftragsverarbeiter:innen für „<i>ein dem Risiko angemessenes Schutzniveau</i>“ zu sorgen haben; ▪ strafrechtliche Bestimmungen, wie etwa die Straftatbestände „Verletzung von Berufsgeheimnissen“ (§ 121 StGB), „Amtsmissbrauch“ (§ 302 StGB) oder „Verletzung eines Amtsgeheimnisses“ (§ 310 StGB). <p>Aufgrund der gegenständlichen Verarbeitung, insbesondere der geltenden, strengen Strafdrohungen ist nicht von erheblichen wirtschaftlichen oder gesellschaftlichen Nachteilen für die betroffenen Personen auszugehen, womit die gegenständliche Anforderung als erfüllt angesehen werden kann.</p>
<p>Nachteile durch Unterbleiben der Verarbeitung (EG 90 iVm 85 DSGVO; WP 248 Rev.01, 21 und 28)</p>	<p><u>Ursache:</u> Sollte die Verarbeitung unterbleiben, sind physische Nachteile für die betroffenen Personen denkbar, weil die Gesundheitsversorgung möglicherweise nicht so gut funktioniert, wie sie funktionieren könnte.</p> <p><u>Art:</u> Theoretisch denkbar sind nicht oder zu spät erkannte Erkrankungen, wenn beispielsweise Screening-Programme nicht zielgerichtet umgesetzt oder nicht nach neuesten wissenschaftlichen Erkenntnissen aufgesetzt werden. Denkbar wären zudem zu späte Behandlungen, in denen Erkrankungen, die bei früherer Erkennung gut heilbar gewesen wären, nur schlecht oder gar nicht mehr geheilt werden können. Allgemein kann ein Unterbleiben der Verarbeitung zu mangelhafter Planung und suboptimal organisierten Versorgungsprozessen (vgl. etwa die evidenzbasierte Gestaltung und Evaluierung von Screening oder Disease Management-Programmen) – und in Folge zu Situationen der Über-, Unter- oder Fehlversorgung führen. Ein Unterbleiben der Verarbeitung kann darüber hinaus zu Situationen führen, in denen eine nicht den medizinischen Leitlinien entsprechende Versorgung erst verspätet erkannt wird.</p> <p><u>Besonderheit:</u> Die Besonderheit des gegenständlichen Risikos ergibt sich daraus, dass es sich nicht um ein Risiko bei Verarbeitung der Daten, sondern bei Unterbleiben der Verarbeitung handelt. Für die gegenständliche Verarbeitung muss dieses Risiko auch auf jeden Fall betrachtet werden, weil die Verarbeitung im wahrsten Sinne des Wortes Menschenleben retten kann, wenn das Gesundheitssystem besser funktioniert. Die Debatte um die Kosten der Nicht-Verwendung von Gesundheitsdaten in der Sekundärnutzung ist eng verbunden mit den Diskussionen um die Begründung eines Europäischen Gesundheitsdatenraumes, dessen Sekundärnutzungsbestimmungen vorallem auf die Verbesserung der Gesundheitspolitik und Systemsteuerung abzielen.</p> <p><u>Schwere:</u> Im schlimmsten Fall können verzögerte Behandlungen bzw. nicht rechtzeitig erkannte Erkrankungen zu schwereren Verläufen oder soagr lebensbedrohlichen Zuständen führen. Es kann auch sein, dass die Heilungschancen wesentlich verschlechtert werden und die Behandlung intensiver und langwieriger wird, was wiederum zu höheren Kosten (nicht nur für die öffentliche Hand) sowie längerem Verdienstentgang führen kann. Auch erhöht sich das Risiko für chronische Zustände und erhöhte psychische Belastungen bei den Betroffenen und ihren Angehörigen. Negative Auswirkungen auf das soziale und berufliche Leben sind ebenso zu erwarten.</p> <p><u>Eintrittswahrscheinlichkeit:</u> Je weniger Daten zur Steuerung, Planung und Evaluierung verarbeitet werden, umso größer ist die Gefahr, dass erforderliche Verbesserungen im österreichischen Gesundheitssystem nicht erkannt und folglich auch nicht umgesetzt werden. Aufgrund der großen Zahl an Betroffenen führt das Unterbleiben der Verarbeitung statistisch gesehen, sicher zu gesundheitlichen Nachteilen für die Bevölkerung, auch wenn diese im Einzelfall nicht zugeordnet werden können.</p> <p>Aufgrund der großen Zahl der Betroffenen und der potenziellen Schwere der Nachteile, die mit dem Unterbleiben der Verarbeitung verbunden sind, kann die gegenständliche Anforderung nur als erfüllt angesehen werden, wenn die Verarbeitung tatsächlich durchgeführt wird (so wie</p>

	<p>dies in der aktuell vorgeschlagenen Fassung des § 11 G-ZG vorgesehen ist).</p>
<p>ABHILFEMASSNAHMEN Als Maßnahmen, Garantien und Verfahren zur Eindämmung von Risiken werden insbesondere in den Erwägungsgründen 28, 78 und 83 DSGVO genannt:</p>	
<p>Minimierung der Verarbeitung personenbezogener Daten (EG 78 und Art. 35 Abs. 7 Buchstabe d DSGVO; WP 248 Rev.01, 21 und 29)</p>	<p>Die Minimierung der Daten erfolgt insbesondere durch die Verwendung von bereichsspezifischen Personenkennzeichen sowie die Beschränkung der Verarbeitungsdauer gemäß § 11 Abs. 4 Z 2 bis 4 G-ZG. Außerdem sollen nur jene Daten verarbeitet werden, die für die Erstellung von Betriebs- und Vollziehungskennzahlen erforderlich sind. In internen Datenschutz-Richtlinien sollen besondere Vorkehrungen wie etwa ein Berechtigungssystem oder ein softwaregestütztes Datenschutz-Management vorgesehen werden.</p> <p>Die Anforderung “Abhilfe durch Minimierung der Verarbeitung personenbezogener Daten” ist insbesondere aufgrund der Verwendung von bereichsspezifischen Personenkennzeichen als erfüllt anzusehen.</p>
<p>Schnellstmögliche Pseudonymisierung personenbezogener Daten (EG 28 und 78 sowie Art. 35 Abs. 7 Buchstabe d DSGVO; WP 248 Rev.01, 21 und 29)</p>	<p>Mit einer Anonymisierung oder Aggregation ist ein hoher Informationsverlust verbunden (<i>Sachverständigenrat</i>, Rn 22). Aus diesem Grund wird die Anonymisierung auch nur für die Bereitstellung von Auswertungen vorgesehen (§ 11 Abs. 4 Z 3 G-ZG). Nach der ständigen Judikatur der Datenschutzbehörde (DSB 30.03.2015, DSB-D215.611/0003-DSB/2014; DSK 22.05.2013, K213.180/0021-DSK/2013) besteht k-Anonymität – und damit kein Personenbezug sowie folglich keine Anwendbarkeit des Datenschutzrechts – für $k > 5$. Dies ist – wie bereits ausgeführt – nur für die Bereitstellung von Auswertungen einzuhalten. Für Die Ausarbeitung von Auswertungen dürfen pseudonymisierte Daten verarbeitet werden. Diese sind diesbezüglich ausreichend, weshalb § 11 Abs. 4 Z 2 G-ZG vorsieht, dass personenbezogene Daten ausschließlich in pseudonymisierter Form unter Verwendung bereichsspezifischer Personenkennzeichen (§ 9 E-GovG) verarbeitet werden dürfen. D.h. bereits die Bereitstellung gemäß § 11 Abs. 3 G-ZG seitens eines der Gesundheits-Zielsteuerungspartner darf nur mit bPK – anstelle des Namens – erfolgen.</p> <p>Vor allem hinsichtlich institutioneller Gesundheitsdiensteanbieter (GDA) wird der Object Identifier (OID) zum Einsatz kommen. Dieser ist einem GDA eindeutig zugeordnet und über das öffentliche OID-Portal auf den GDA rückführbar. Die Verwendung von bereichsspezifischen Personenkennzeichen ist in der Praxis nicht (immer) möglich, weil diese nicht vollständig bzw. flächendeckend im GDA-Index vorhanden sind.</p> <p>Die Anforderung “Abhilfe durch schnellstmögliche Pseudonymisierung” ist aufgrund der Anforderung gemäß § 11 Abs. 4 Z 3 des Gesundheits-Zielsteuergesetzes in der vorgeschlagenen Fassung als erfüllt anzusehen.</p>
<p>Transparenz in Bezug auf die Funktionen und die Verarbeitung personenbezogener Daten (EG 78 DSGVO und Art. 35 Abs. 7 Buchstabe d DSGVO; WP 248 Rev.01, 21 und 29)</p>	<p>Durch die Publikation des Gesundheits-Zielsteuergesetzes als Bundesgesetz im Bundesgesetzblatt sowie der parlamentarischen Materialien im Zuge des Gesetzgebungsprozesses können die Hintergründe von der Öffentlichkeit kostenlos nachvollzogen werden. Außerdem wird die erforderliche Datenschutzerklärung im Internet zur Verfügung gestellt werden. Auch die allfällige Einrichtung einer Anlaufstelle gemäß Art. 26 DSGVO seitens der Gesundheits-Zielsteuerungspartner würde die Transparenz für die betroffenen Personen erhöhen.</p> <p>Die Anforderung “Abhilfe durch Transparenz in Bezug auf die Funktionen und die Verarbeitung personenbezogener Daten” ist aufgrund der grundsätzlichen Machbarkeit als erfüllbar anzusehen.</p>

<p>Überwachung der Verarbeitung personenbezogener Daten durch die betroffenen Personen <small>(EG 78 DSGVO und Art. 35 Abs. 7 Buchstabe d DSGVO; WP 248 Rev.01, 21 und 29)</small></p>	<p>Auf Grundlage der Datenschutz-Grundverordnung stehen natürlichen Personen folgende Rechte gegenüber den Gesundheits-Zielsteuerungspartnern zu:</p> <ul style="list-style-type: none"> ▪ das Recht auf Auskunft (Art. 15 DSGVO), ▪ das Recht auf Berichtigung (Art. 16 DSGVO) sowie ▪ das Recht auf Einschränkung der Verarbeitung (Art. 18 DSGVO). <p>Diese Rechte können gegenüber den Verantwortlichen, d.h. den Gesundheits-Zielsteuerungspartnern, geltend gemacht werden.</p> <p>Die Anforderung “Abhilfe durch Überwachung der Verarbeitung personenbezogener Daten durch die betroffenen Personen” ist aufgrund der grundsätzlichen Machbarkeit als erfüllbar anzusehen.</p>
<p>Datensicherheitsmaßnahmen <small>(EG 78 und 83 DSGVO sowie Art. 35 Abs. 7 Buchstabe d DSGVO; WP 248 Rev.01, 21 und 29)</small></p>	<p>Grundsätzlich sind auf die IT-Systeme der Gesundheits-Zielsteuerungspartner die Vorgaben des Österreichischen Informationssicherheitshandbuchs (siehe: https://www.sicherheitshandbuch.gv.at/) anwendbar. Diese sehen u.a. Richtlinien zu den folgenden Themen vor:</p> <ul style="list-style-type: none"> ▪ Informationssicherheitsmanagementsystem (ISMS) ▪ Managementverantwortung und Aufgaben beim ISMS ▪ Risikoanalyse ▪ Informationssicherheitspolitik ▪ Organisation ▪ Personelle Sicherheit ▪ Vermögenswerte und Klassifizierung von Informationen ▪ Zugriffskontrolle, Berechtigungssysteme, Schlüssel- und Passwortverwaltung ▪ Kryptographie ▪ Physische und umgebungsbezogene Sicherheit ▪ Sicherheitsmanagement im Betrieb ▪ Sicherheitsmanagement in der Kommunikation ▪ Sicherheit in Entwicklung, Betrieb und Wartung eines IT-Systems ▪ Lieferantenbeziehungen ▪ Sicherheitsvorfälle bzw. Informationssicherheitsereignisse (Incident Handling) ▪ Disaster Recovery und Business Continuity ▪ Security Compliance ▪ Sicherheitsszenarien ▪ Sicherheitstechnologien ▪ Cloud Computing ▪ Smartphone Sicherheit ▪ Sicherheit in Sozialen Netzen ▪ Sichere Beschaffung ▪ Muster für Verträge, Verpflichtungserklärungen und Dokumentationen <p>Bereits im aktuellen Entwurf sind folgende technische und organisatorische Maßnahmen grundgelegt:</p> <ul style="list-style-type: none"> ▪ die Verschwiegenheitspflicht für alle an der Verarbeitung beteiligten Personen (§ 11 Abs. 4 Z 1 G-ZG); ▪ die ausschließliche Verarbeitung unter Verwendung bereichsspezifischer Personenkennzeichen (§ 11 Abs. 4 Z 2 G-ZG); ▪ die Beschränkung der Empfänger von Primärdaten auf Gesundheits-Zielsteuerungspartner (§ 11 Abs. 4 Z 3 G-ZG); ▪ die Pflicht zur Löschung der Primärdaten nach Erstellung der Auswertungen (§ 11 Abs. 4 Z 4 G-ZG); ▪ die Protokollierung der einzelnen Verarbeitungsschritte (§ 11 Abs. 4 Z 5 G-ZG).

	<p>Die Anforderung “Abhilfe durch Datensicherheitsmaßnahmen” ist aufgrund der umfangreichen geplanten sowie bereits im Gesundheits-Zielsteuerungsgesetz vorgesehenen Datensicherheitsmaßnahmen als erfüllbar anzusehen.</p>
<p>BERÜCKSICHTIGUNG VON DATENSCHUTZINTERESSEN Gemäß Art. 35 Abs. 2 und 9 sowie Art. 36 Abs. 4 DSGVO ist – wenn möglich – der Rat des Datenschutzbeauftragten einzuholen und sind die betroffenen Personen anzuhören:</p>	
<p>Stellungnahme des Datenschutzbeauftragten (Art. 35 Abs. 2 DSGVO; WP 248 Rev.01, 21 und 29)</p>	<p>Die Stellungnahmen der datenschutzbeauftragten Personen der Gesundheits-Zielsteuerungspartner können eingeholt werden.</p> <p>Die Anforderung “Stellungnahme des Datenschutzbeauftragten” ist aufgrund der grundsätzlichen Machbarkeit als erfüllbar anzusehen.</p>
<p>Stellungnahme betroffener Personen (Art. 35 Abs. 9 DSGVO; WP 248 Rev.01, 21 und 29)</p>	<p>Die Stellungnahmen von betroffenen Personen oder ihren Vertretungen, wie etwa Patient:innenanwält:innen, können eingeholt werden.</p> <p>Die Anforderung “Stellungnahme betroffener Personen” ist aufgrund der grundsätzlichen Machbarkeit der Einholung von Stellungnahmen als erfüllbar anzusehen.</p>