DOKUMENTATIONS- UND INFORMATIONSYSTEM FÜR ANALYSEN IM GESUNDHEITSWESEN – DIAG (BUNDESGESETZ ÜBER DIE DOKUMENTATION IM GESUNDHEITSWESEN)

Die folgende Datenschutz-Folgenabschätzung (DSFA) betrifft das Dokumentations- und Informationssystem für Analysen im Gesundheitswesen (DIAG) zur Steuerung des Gesundheitswesens gemäß dem Bundesgesetz über die Dokumentation im Gesundheitswesen.

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 (im Bundesgesetz über die Dokumentation im Gesundheitswesen) 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 des Bundesgesetzes über die Dokumentation im Gesundheitswesen 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	Datenschutz-beauftragter
Umfang der Verar-beitung	eindeutiger Zweck	Kontrollverlust	Pseudonymisierung	betroffene Personen
Kontext der Verar-beitung	legitimer Zwecke	Diskriminierung	Transparenz	
Zweck der Verarbei-tung	Rechtmäßigkeit	Identitätsdiebstahl & -betrug	Überwachung	
personenbezogene Daten	Angemessenheit	Finanzielle Verluste	Datensicherheits-maßnahmen	
Empfänger:innen	Erheblichkeit	unbef Aufhebung Pseudonymisierung		
Speicherdauer	Beschränktheit auf notwendiges Maß	Rufschädigung		
funktionelle Be-schreibung	Speicherbegrenzung	Verlust Berufsge-heimnisse		
Hard- und Software	generelle Informatio-nen	gesellschaftliche Nachteile		
Verhaltensregeln	Informationen (Art 13 DSGVO)	(Risiken bei Unter-bleiben)		
	Informationen (Art 14 DSGVO)			
	Auskunft & Daten-übertragbarkeit			
	Berichtigung & Lö-schung			
	Widerspruch & Ein-schränkung			
	Auftrags-verarbeiter:innen		**Legende**	erfüllt
	Übermittlung in Drittländer			erfüllbar
	vorherige Konsulta-tion			nicht erfüllt

SYSTEMATISCHE BESCHREIBUNG der geplanten Verarbeitungsvorgänge, Zwecke sowie berechtigten Interessen *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:*	
Art der Verarbeitung (EG 90 DSGVO; WP 248 Rev.01, 21 und 28)	Die Verarbeitung erfolgt elektronisch im Rahmen einer Server-Client-Applikation. 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 (*Art-29-Datenschutzgruppe*, WP 248 Rev.01, 8) zu versorgen. Verantwortliche für das DIAG im Sinne des Art. 4 Nr. 7 DSGVO ist die Gesundheitsminister:in (§ 4 Abs. 3 des Bundesgesetzes über die Dokumentation im Gesundheitswesen). **Die Anforderung "Beschreibung der Art der Verarbeitung" ist aufgrund der angeführten Beschreibung als erfüllt anzusehen.**
Umfang der Verarbeitung (EG 90 DSGVO; WP 248 Rev.01, 21 und 28)	Das DIAG umfasst potenziell alle Personen, die mit dem österreichischen Gesundheitswesen – egal in welcher Rolle – in Berührung kommen. In geografischer Sicht umfasst das DIAG das gesamte Bundesgebiet, weil die evidenzbasierte Planung und Steuerung des österreichischen Gesundheitswesens ermöglicht werden soll. Das DIAG stellt bereits aufgrund des geographischen Ausmaßes einen großen Umfang im Sinne der Art-29-Datenschutzgruppe (WP 248, 11) dar. **Die Anforderung "Beschreibung des Umfangs der Verarbeitung" ist aufgrund der angeführten Beschreibung als erfüllt anzusehen.**
Kontext der Verarbeitung (EG 90 DSGVO; WP 248 Rev.01, 21 und 28)	Die Verarbeitung erfolgt im Kontext der Planung und Steuerung des österreichischen Gesundheitssystems, genauer gesagt zur Erreichung der unten im Feld „BESCHREIBUNG / Zweck der Verarbeitung" näher beschriebenen Zwecke. Das DIAG setzt die folgenden Verarbeitungen voraus, deren Ergebnisse in das DIAG einfließen: ▪ Diagnosen- und Leistungsdokumentation im stationären Bereich (Hauptstück A), die gemäß § 2 Abs. 3 des Bundesgesetzes über die Dokumentation im Gesundheitswesen folgende Daten umfasst: – Diagnosen (im Format gemäß § 1a Abs. 1 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); – medizinischen Leistungen auf Basis der LKF (§ 1a Abs. 2 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); – administrative Daten, wie etwa Datum und Art der Aufnahme, Datum und Art der Entlassung, Krankenanstaltennummer, Aufnahmezahl, Geburtsdatum, Geschlecht, Postleitzahl, Gemeindecode (§ 4 Z 1 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); – medizinische Daten, d.h. Haupt- und Zusatzdiagnose, ausgewählte medizinische Leistungen sowie Verlegungen innerhalb der Krankenanstalt (§ 4 Z 2 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ Diagnosen- und Leistungsdokumentation im ambulanten Bereich (Hauptstück B), die gemäß § 6 Abs. 3 des Bundesgesetzes über die Dokumentation im Gesundheitswesen folgende Daten umfasst: – Diagnosen (im Format gemäß § 6 Abs. 1 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); – medizinischen Leistungen (in einem praxisorientierten, leicht

	administrierbaren Leistungskatalogformat [§ 6 Abs. 1 des Bundesgesetzes über die Dokumentation im Gesundheitswesen]); – Angaben zu seltenen Erkrankungen durch Angabe der Orpha-Kennnummer, allerdings nur wenn die Leistungserbringer:in eine Krankenanstalt ist (§ 6a Abs. 2 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); – Angaben zur Patient:in, wie insbesondere Altersgruppe zum Kontaktzeitpunkt, Geschlecht, Staatsbürgerschaft, Wohnsitz (Staat, Postleitzahl und Gemeindecode), bereichsspezifische Personenkennzeichen (§ 6 Abs. 3 Z 1 des Bundesgesetzes über die Dokumentation im Gesundheitswesen) sowie die Sozialversicherungsnummer, wenn die Leistungserbringer:in eine niedergelassene Ärzt:in, eine Gruppenpraxis oder ein selbständiges Ambulatorium ist (§ 6a Abs. 3 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); – Angaben zur Leistungserbringer:in, wie insbesondere (Leistungserbringer:in-)Identifikationsnummer und OID gemäß eHVD, Abteilungsfunktionscode bzw. Fachgebiet, Berufssitz (Postleitzahl, Gemeindecode), Organisationsform, Kostenstellenplan (§ 6 Abs. 3 Z 2 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); – Angaben zum ambulanten Kontakt; ▪ Dokumentation von Statistik- und Kostendaten in Krankenanstalten (Hauptstück C), gemäß § 7 und § 8 des Bundesgesetzes über die Dokumentation im Gesundheitswesen; ▪ weitere Daten (Hauptstück D), die gemäß § 9a des Bundesgesetzes über die Dokumentation im Gesundheitswesen folgende Daten umfassen: – Informationen zur Todesursache aus der Todesursachenstatistik der Bundesanstalt „Statistik Österreich“ (§ 9a Abs. 1 Z 1 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); – bPK GH der verstorbenen Person (§ 9a Abs. 1 Z 2 des Bundesgesetzes über die Dokumentation im Gesundheitswesen). Die Diagnosen- und Leistungsdokumentationen im stationären Bereich (Hauptstück A) sind von den Trägern der Krankenanstalten im Wege der Landeshauptleute bzw. direkt an das DIAG bereitzustellen (§ 2 des Bundesgesetzes über die Dokumentation im Gesundheitswesen). Die Diagnosen- und Leistungsdokumentationen im ambulanten Bereich (Hauptstück C) sind von ▪ den Trägern der Krankenanstalten, die über Landesgesundheitsfonds abgerechnet werden, im Wege der Landesgesundheitsfonds (§ 6a Abs. 1 des Bundesgesetzes über die Dokumentation im Gesundheitswesen) ▪ den Landesgesundheitsfonds, ▪ dem Dachverband der österreichischen Sozialversicherungsträger, ▪ den Trägern der Krankenfürsorgeanstalten im Wege des Dachverbands der österreichischen Sozialversicherungsträger, ▪ niedergelassenen Ärzt:innen direkt (ohne Kassenvertrag) oder im Wege der Abrechnung über den Dachverband (mit Kassenvertrag), ▪ Gruppenpraxen, direkt (ohne Kassenvertrag) oder im Wege der Abrechnung über den Dachverband (mit Kassenvertrag), sowie ▪ selbständigen Ambulatorien, direkt (ohne Kassenvertrag) oder im Wege der Abrechnung über den Dachverband (mit Kassenvertrag), an das DIAG bereitzustellen (§ 6 Abs. 3 des Bundesgesetzes über die Dokumentation im Gesundheitswesen). Die Statistik- und Kostendatendokumentation im intramuralen Bereich sind von den Trägern der Krankenanstalten im Wege der Landeshauptleute bzw. direkt an das DIAG bereitzustellen (§§ 7 und 8 des Bundesgesetzes über die Dokumentation im Gesundheitswesen). Die Todesursachen sind von der Bundesanstalt „Statistik Österreich“ direkt an

	das DIAG bereitzustellen (§ 9a des Bundesgesetzes über die Dokumentation im Gesundheitswesen). Das DIAG wiederum stellt den unten im Feld „BESCHREIBUNG / Empfänger:innen“ angeführten Empfänger:innen die im DIAG enthaltenen Daten bereit, soweit diese für die Wahrnehmung gesetzlicher Aufgaben durch die Empfänger:innen erforderlich sind. **Die Anforderung “Beschreibung des Kontexts der Verarbeitung” ist aufgrund der angeführten Beschreibung als erfüllt anzusehen.**
Zweck der Verarbeitung (EG 90 sowie Art. 35 Abs. 7 Buchstabe a DSGVO; WP 248 Rev.01, 21 und 28)	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). Zu deren Einhaltung müssen die obersten Organe, d.h. u.a. auch die Gesundheitsminister:in, effektiv Steuerungs- und Lenkungsfunktionen wahrnehmen; können sie dies nicht, sind entgegenstehende einfachgesetzliche Bestimmungen verfassungswidrig (VfSlg. 17.421/2004). Zur Wahrnehmung der Steuerungs- und Lenkungsfunktionen 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). 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). Nach Erwägungsgrund 32 DSGVO können Verarbeitungen auch mehreren Zwecken dienen. Dies ist im gegebenen Zusammenhang der Fall, da das DIAG ▪ der Steuerung des Gesundheitswesens (§ 1 Z 1 und § 6 Abs. 2 des Bundesgesetzes über die Dokumentation im Gesundheitswesen), ▪ der Evaluierung von gesundheitspolitischen und Public Health-Aktivitäten (§ 1 Z 2 des Bundesgesetzes über die Dokumentation im Gesundheitswesen), ▪ der Qualitätssicherung (§ 1 Z 2 und § 6 Abs. 2 des Bundesgesetzes über die Dokumentation im Gesundheitswesen), ▪ der sektorenübergreifen Dokumentation (§ 1 Z 3 des Bundesgesetzes über die Dokumentation im Gesundheitswesen) sowie ▪ der Implementierung, Durchführung und Beobachtung der partnerschaftlichen Zielsteuerung-Gesundheit (§ 1 Z 4 des Bundesgesetzes über die Dokumentation im Gesundheitswesen) dient. **Die Anforderung “Beschreibung des Zwecks der Verarbeitung” ist aufgrund der angeführten Beschreibung als erfüllt anzusehen.**
Personenbezogene Daten (WP 248 Rev.01, 21 und 28)	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. Die verarbeiteten Daten entsprechen den oben im Feld „BESCHREIBUNG / Kontext der Verarbeitung“ beschriebenen Datenarten. **Die Anforderung “Beschreibung der personenbezogenen Daten” ist aufgrund der oben im Feld „BESCHREIBUNG / Kontext der Verarbeitung“ beschriebenen Datenarten jedenfalls als erfüllt anzusehen.**

Empfänger:innen (EG 90 DSGVO; WP 248 Rev.01, 21 und 28)	Daten aufgrund des Bundesgesetzes über die Dokumentation im Gesundheitswesen werden u.a. an folgende Empfänger:innen übermittelt: ▪ Bundesanstalt „Statistik Österreich“ (§ 5 Abs. 1 des Bundesgesetzes über die Dokumentation im Gesundheitswesen) ▪ Dachverband der österreichischen Sozialversicherungsträger (§ 5 Abs. 2 und § 6e Abs. 1 des Bundesgesetzes über die Dokumentation im Gesundheitswesen) ▪ Sozialversicherungsträger (§ 5 Abs. 2 und § 6e Abs. 1 des Bundesgesetzes über die Dokumentation im Gesundheitswesen) ▪ Bundesgesundheitsagentur (§ 5 Abs. 3 und § 6e Abs. 2 des Bundesgesetzes über die Dokumentation im Gesundheitswesen) ▪ Landesgesundheitsfonds (§ 5 Abs. 3 und § 6e Abs. 2 des Bundesgesetzes über die Dokumentation im Gesundheitswesen) ▪ Länder (§ 5 Abs. 3 und § 6e Abs. 2 des Bundesgesetzes über die Dokumentation im Gesundheitswesen) **Die Anforderung “Beschreibung der Empfänger:innen” ist aufgrund der angeführten Beschreibung als erfüllt anzusehen.**
Speicherdauer (WP 248 Rev.01, 21 und 28)	Eine Mindestspeicherdauer ist gesetzlich nicht vorgesehen. Dafür sind zwei Löschfristen ist in § 4 Abs. 5 des Bundesgesetzes über die Dokumentation im Gesundheitswesen vorgesehen und zwar: ▪ Löschung von Pseudonymen, insbesondere bereichsspezifischen Personenkennzeichen (diese sind nach Ansicht der Datenschutzkommission [Vorgängerbehörde der Datenschutzbehörde] als Pseudonyme anzusehen: DSK 22.5.2013, K202.126/0012-DSK/2013), nach 15 Jahren sowie ▪ Löschung aller anderer Daten nach weiteren 10 d.h. insgesamt 25 Jahren. Die Löschpflicht des § 4 Abs. 5 des Bundesgesetzes über die Dokumentation im Gesundheitswesen gilt gemäß § 5 Abs. 1 des Bundesgesetzes über die Dokumentation im Gesundheitswesen auch gegenüber der Bundesanstalt „Statistik Österreich“ und gemäß § 5 Abs. 4 des Bundesgesetzes über die Dokumentation im Gesundheitswesen auch gegenüber allen sonstigen Empfänger:innen. **Die Anforderung “Beschreibung der Speicherdauer” ist aufgrund der angeführten Beschreibung als erfüllt anzusehen.**
Funktionelle Beschreibung der Verarbeitungsvorgänge (WP 248 Rev.01, 21 und 28)	Das DIAG umfasst folgende Funktionen: ▪ DIAG-Daten empfangen: Die Landeshauptleute, die Landesgesundheitsfonds, die Träger von Krankenanstalten, die nicht über Landesgesundheitsfonds abgerechnet werden, der Dachverband der österreichischen Sozialversicherungsträger, die Träger der Krankenfürsorgeanstalten, die niedergelassenen Ärzt:innen, die Gruppenpraxen, die selbständigen Ambulatorien sowie die Bundesanstalt „Statistik Österreich“ sind nach den Bestimmungen des Bundesgesetzes über die Dokumentation im Gesundheitswesen zur Übermittlung von Daten verpflichtet, die seitens der Gesundheitsminister:in für Zwecke des DIAG zu empfangen sind (siehe näher dazu – oben Feld „BESCHREIBUNG / Kontext der Verarbeitung“). ▪ DIAG-Auswertungen erstellen: Für die in § 1 des Bundesgesetzes über die Dokumentation im Gesundheitswesen beschriebenen Zwecke, insbesondere der Planung, Steuerung und zur Sicherstellung einer gesamthaften Finanzierung des österreichischen Gesundheitswesens können Auswertungen erstellt werden. ▪ DIAG-Daten übermitteln: Soweit dies zur Wahrnehmung ihrer gesetzlich übertragenen Aufgaben erforderlich ist sind den Ländern, den Landesgesundheitsfonds, der Bundesgesundheitsagentur, dem Dachverband der österreichischen Sozialversicherungsträger, den Sozialversicherungsträgern sowie der Bundesanstalt „Statistik Österreich“ die DIAG-Daten bereitzustellen (siehe näher dazu – oben Feld „BESCHREIBUNG / Empfänger:innen“).

	▪ DIAG-Daten löschen: Die DIAG-Daten sind nach 15 bzw. 25 Jahren zu löschen (siehe näher dazu – oben Feld „BESCHREIBUNG / Speicherdauer“). **Die Anforderung “Funktionelle Beschreibung der Verarbeitungsvorgänge” ist aufgrund der angeführten Beschreibung als erfüllt anzusehen.**
Beschreibung der Hard- und Software bzw. sonstigen Infrastruktur (WP 248 Rev.01, 21 und 28)	Da die im vorliegenden Entwurf vorgesehen Änderungen erst umzusetzen sind, sind hinsichtlich der genauen Beschreibung der Infrastruktur noch allfällige Ausschreibungen abzuwarten. **Die Anforderung “Beschreibung der Hard- und Software bzw. sonstigen Infrastruktur” ist aufgrund der angeführten Beschreibung als erfüllbar anzusehen.**
Eingehaltene, gemäß Art. 40 DSGVO genehmigte Verhaltensregeln (Art. 35 Abs. 8 DSGVO; WP 248 Rev.01, 21 und 28)	Das Instrument der Verhaltensregeln ist für Behörden und öffentliche Stellen nicht anwendbar (Art. 41 Abs. 6 DSGVO bzw. mwN *Schweinoch*/*Will* in *Ehmann*/*Selmayr*, DSGVO[2] Art. 40-43 Rn. 10). Da das DIAG allerdings von erheblichem öffentlichen Interesse ist (näher dazu – siehe unten: BEWERTUNG / Rechtmäßigkeit der Verarbeitung) sollen als Folge dieser Datenschutz-Folgenabschätzung verwaltungsinterne Erlässe und Rundschreiben sowie allgemeine verfügbare Datenschutzinformationen, wie etwa die Datenschutzerklärung, aktualisiert bzw. ausgearbeitet werden. **Die Anforderung “Beschreibung der eingehaltenen, gemäß Art 40 genehmigten Verhaltensregeln” ist aufgrund der angeführten Beschreibung als erfüllbar anzusehen.**
BEWERTUNG der Notwendigkeit und Verhältnismäßigkeit *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 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.*	
Festgelegter Zweck (EG 90 und Art. 35 Abs. 7 Buchstabe b DSGVO; WP 248 Rev.01, 21 und 28)	Die Zwecke der Verarbeitung sind in § 1 des Bundesgesetzes über die Dokumentation im Gesundheitswesen wie folgt festgelegt: ▪ Steuerung des Gesundheitswesens (§ 1 Z 1 und § 6 Abs. 2 des Bundesgesetzes über die Dokumentation im Gesundheitswesen), ▪ Evaluierung von gesundheitspolitischen und Public Health-Aktivitäten (§ 1 Z 2 des Bundesgesetzes über die Dokumentation im Gesundheitswesen), ▪ Qualitätssicherung (§ 1 Z 2 und § 6 Abs. 2 des Bundesgesetzes über die Dokumentation im Gesundheitswesen), ▪ sektorenübergreife Dokumentation (§ 1 Z 3 des Bundesgesetzes über die Dokumentation im Gesundheitswesen) sowie ▪ Implementierung, Durchführung und Beobachtung der partnerschaftlichen Zielsteuerung-Gesundheit (§ 1 Z 4 des Bundesgesetzes über die Dokumentation im Gesundheitswesen). **Die Anforderung “Bewertung der Festlegung des Zwecks” ist aufgrund der ausdrücklichen, gesetzlichen Festlegung des Zwecks in § 1 des Bundesgesetzes über die Dokumentation im Gesundheitswesen als erfüllt anzusehen.**
Eindeutiger Zweck (Art. 35 Abs. 7 Buchstabe b iVm Art. 5 Abs. 1 Buchstabe b DSGVO; WP 248 Rev.01, 21 und 28)	Die Zwecke sind in § 1 des Bundesgesetzes über die Dokumentation im Gesundheitswesen eindeutig festgelegt. **Die Anforderung “Bewertung der Eindeutigkeit des Zwecks” ist aufgrund**

	der ausdrücklichen, gesetzlichen Festlegung des Zwecks in § 1 des Bundesgesetzes über die Dokumentation im Gesundheitswesen als erfüllt anzusehen.
Legitimer Zweck (Art. 35 Abs. 7 Buchstabe b iVm Art. 5 Abs. 1 Buchstabe b DSGVO; WP 248 Rev.01, 21 und 28)	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. 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 Lenkungsfunktionen 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 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: *„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.“* Die vom EuGH zitierte Bestimmung des Art. 24 Abs. 1 Unterabs. 2 der Durchführungsverordnung 2015/2447 lautet: *„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:* *a) der Antragsteller;* *b) die Person, die für das antragstellende Unternehmen verantwortlich ist oder die Kontrolle über seine Leitung ausübt;* *c) der Beschäftigte des Antragstellers, der für dessen Zollangelegenheiten*

	zuständig ist." 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. **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 § 1 des Bundesgesetzes über die Dokumentation im Gesundheitswesen sowie im Lichte der einschlägigen EuGH- und VfGH-Judikatur, als erfüllt anzusehen.**
Rechtmäßigkeit der Verarbeitung (Art. 35 Abs. 7 Buchstabe b iVm Art. 6 und 9 DSGVO; WP 248 Rev.01, 21 und 28)	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 ▪ 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 – 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. z.B. Empfehlung 40 im Rechnungshofbericht Reihe Bund 2021/43 zu Gesundheitsdaten zur Pandemiebewältigung); ▪ 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). 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. 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 vorgesehen wirkungsorientierte Verwaltung setzt also die Steuerung nach beabsichtigten Wirkungen und Leistungen voraus. Welche Wirkungen und Leistungen beabsichtigt sind, ist den jeweiligen Materiengesetzen 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. 16 Abs. 5 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 Rechtform, 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 das DIAG aufgrund der umfangreichen Regelung im Bundesgesetz über die Dokumentation im Gesundheitswesen wesentlich strenger determiniert als die der Entscheidung VfSlg. 16.369/2001 zugrundeliegende Bestimmung. Die Regelungen des Bundesgesetzes über die Dokumentation im Gesundheitswesen 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 den Bestimmung des Bundesgesetzes über die Dokumentation im Gesundheitswesen 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 Bundesgesetzes über die Dokumentation im Gesundheitswesen: die darin geregelten Daten stehen schlichtweg nicht zur Verfügung und können auch nicht durch gelindere Mittel als die äußerst schonend vorgesehene, maximal indirekt personenbezogene Verarbeitung erstellt werden. 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 Vorhersehrbarkeit 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). 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 Bundesministeriengesetz 1986 stellen die Bestimmungen des Bundesgesetzes über die Dokumentation im Gesundheitswesen 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 Bundesministeriengesetz 1986 stellt sich zusammengefassst wir folgt dar: ▪ Bestimmungen des Bundesministeriengesetzes 1986 alleine stellen keine eigenständige Eingriffsermächtigung dar (DSB 12.04.2019, DSB-D123.591/0003-DSB/2019). ▪ Bestimmungen des Bundesministeriengesetzes 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). **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.**
Angemessenheit der Verarbeitung (Art. 35 Abs. 7 Buchstabe b iVm Art. 5 Abs. 1 Buchstabe c DSGVO; WP 248 Rev.01, 21 und 28)	Die Verarbeitung ist vor allem deswegen angemessen, weil umfangreiche technische und organisatorische Maßnahmen insbesondere in § 4 Abs. 3 des Bundesgesetzes über die Dokumentation im Gesundheitswesen, wie etwa Zugrifssbeschränkungen und Datenminimierungen, zwingend vorgeschrieben sind. Außerdem ist die Verarbeitung angemessen, weil Datenschutz zur Vermeidung der „*Erschwerung der Verwaltungsführung*“ 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 Datenschutzes ergibt sich aus der Verarbeitungstätigkeit selbst; ebenso die Vermeidung der Erschwerung der Verwaltungsführung, indem mit dem DIAG eine elektronisch optimierte Evidenzbasierung und Evaluierung möglich sein wird, um beispielsweise die Zahl der für Pandemie- und Nicht-Pandemie-Patient:innen verfügbaren Betten und des verfügbaren Personals möglichst genau und auf Knopfdruck feststellen zu können (*Rechnungshof*, Gesundheitsdaten zur Pandemiebewältigung im ersten Jahr der COVID-19-Pandemie, Reihe BUND 2021/43, TZ 19.2). **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.**
Erheblichkeit der	Die Verantwortlichkeit der obersten Organe stellt einen „*Grundgedanken der*

Verarbeitung (Art. 35 Abs. 7 Buchstabe b iVm Art. 5 Abs. 1 Buchstabe c DSGVO; WP 248 Rev.01, 21 und 28)	*Verfassung*“ dar (VfSlg. 3054/1956). Zu deren Einhaltung müssen die obersten Organe, d.h. u.a. auch die Gesundheitsminister:in effektiv Steuerungs- und Lenkungsfunktionen 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). Auch darf das Sachlichkeitsgebot gemäß Art. 7 B-VG nicht übersehen werden: Demnach ist es dem einfachen Gesetzgeber verwehrt, unsachliche Bestimmungen zu erlassen. Aus „*gesundheits- und präventionspolitischen Gründen [ist es beispielsweise] erforderlich, ein Mindestmaß an wissenschaftlichen Informationen zu […] Produkten für die zuständigen Behörden zu erlangen*“ (VfSlg. 20.151/2017). 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 Verfügbarkeit von steuerungsrelevanten Datensets die Herausforderung, sondern deren Verknüpfbarkeit. Eine rezente Überblicksarbeit zum Thema Datenverknüpfbarkeit für eivdenzbasierte Gesundheitspolitik zeigt Ansätze für die Umsetzung von Policy-orientierter Datenverknüpfung (*Panteli et al*, Health and Care Data – Approaches to data linkage for evidence-informed policy). Eine verbesserte Verknüpfbarkeit verbessert die Steuerung, welche wieder eine bessere Gesundheitsversorgung zu geringeren Kosten ermöglicht. Die Verarbeitung ist somit erheblich, weil ohne die Auswertungen des DIAG die Gesundheitsminister:in 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). Ähnich 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 statt dessen 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 grundrechteschonenderen Weg der Pandemiebekämpfung eröffnet.*

	Die Anforderung "Bewertung der Erheblichkeit der Verarbeitung" ist als erfüllt anzusehen, weil die auf Basis des DIAG durchgeführten Auswertungen *conditio sine qua non* für eine verfassungsrechtlich erforderliche Steuerung sind.
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)	Die Einhaltung des Datenminimierungsgrundsatzes gemäß Art. 5 Abs. 1 Buchstabe c DSGVO ist gegeben, weil ▪ die Zugriffe auf das DIAG auf Mitarbeiter:innen des Gesundheitsministeriums beschränkt sind (§ 4 Abs. 3 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ der Zugriff auf Rohdaten und Pseudonyme nur insoweit erteilt werden darf, als dies eine wesentliche Voraussetzung zur Wahrnehmung einer gesetzlich übertragenen Aufgabe ist (§ 4 Abs. 3 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ Analyst:innen vom Zugriff auf Rohdaten und Pseudonyme ausgeschlossen sind (§ 4 Abs. 3 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ bereichsspezifische Personenkennzeichen und sonstige Pseudonyme nach 15 Jahren zu löschen sind (§ 4 Abs. 5 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ alle übrigen Daten nach 25 Jahren zu löschen sind (§ 4 Abs. 5 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ die Pflicht zur Einhaltung der Löschfristen gemäß § 4 Abs. 5 des Bundesgesetzes über die Dokumentation im Gesundheitswesen auch für die Bundesanstalt „Statistik Österreich" gilt (§ 5 Abs. 1 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ die Pflicht zur Einhaltung der Löschfristen gemäß § 4 Abs. 5 des Bundesgesetzes über die Dokumentation im Gesundheitswesen auch für sonstige Empfänger:innen gilt (§ 5 Abs. 4 und § 6e Abs. 3 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ eine Pseudonymisierung durch die Pseudonymisierungsstelle des Dachverbands der österreichischen Sozialversicherungsträger vorgenommen wird (§ 5a des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ der ambulante Bereichs spätestens ab 1. Jänner 2025 verpflichtet ist, gemäß § 6 Abs. 1 des Bundesgesetzes über die Dokumentation im Gesundheitswesenzu codieren; ▪ Aufnahmezahlen durch nicht rückrechenbare Datensatz-IDs und Geburtsdaten durch Altersgruppen zu ersetzen sind (§ 6a Abs. 1 und § 6b des Bundesgesetzes über die Dokumentation im Gesundheitswesen). Hinsichtlich der Erforderlichkeit der Verarbeitung der umfassten Daten darf oben auf Feld „BEWERTUNG / Erheblichkeit der Verarbeitung" verwiesen werden. Zusätzlich ist vorgesehen, die Einhaltung des Datenminimierungsgrundsatzes durch entsprechende Strategie-Dokumente, wie etwa einer internen Datenschutz-Richtlinie jederzeit belegen zu können. **Die Anforderung "Bewertung der Beschränktheit der Verarbeitung auf das notwendige Maß" ist als erfüllt anzusehen, insbesondere, weil weitgehende Ein- und Beschränkungen der Verbeitungstätigkeit „DIAG" im Bundesgesetz über die Dokumentation im Gesundheitswesen vorgesehen sind.**
Speicherbegrenzung (Art. 5 Abs. 1 Buchstabe e DSGVO; WP 248 Rev.01, 21 und 28)	Wie bereits oben im Feld „SYSTEMATISCHE BESCHREIBUNG / Speicherdauer" ausgeführt, bestehen 15- bis 25-jährige Löschfristen. **Durch diese ausdrückliche Löschpflicht ist die Anforderung "Bewertung der Speicherbegrenzung" als erfüllt anzusehen, weil Maßnahmen zur Begrenzung der Speicherdauer ausdrücklich gesetzlich vorgeschrieben sind.**

Generelle Information der betroffenen Personen (Art. 12 DSGVO; WP 248 Rev.01, 21 und 28)	Eine Datenschutzerklärung liegt für die gegenständliche Verarbeitung noch nicht vor. 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. **Die Anforderung "Bewertung der Information der betroffenen Personen bei Erhebung" ist aufgrund der grundsätzlichen Machbarkeit einer solchen Information als erfüllbar anzusehen.**
Information der betroffenen Personen bei Erhebung (Art. 13 DSGVO; WP 248 Rev.01, 21 und 28)	Eine Datenschutzerklärung liegt für die gegenständliche Verarbeitung noch nicht vor. Zur Einhaltung der klaren und einfachen Sprache – siehe oben: Feld „BEWERTUNG / Generelle Informationen der betroffenen Personen". **Die Anforderung "Bewertung der Information der betroffenen Personen bei Erhebung" ist aufgrund der grundsätzlichen Machbarkeit einer solchen Information als erfüllbar anzusehen.**
Information der betroffenen Personen, wenn die Daten nicht bei ihnen erhoben werden (Art. 14 DSGVO; WP 248 Rev.01, 21 und 28)	Siehe oben: Feld „BEWERTUNG / Information der betroffenen Personen bei Erhebung". **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.**
Auskunftsrecht der betroffenen Personen und Recht auf Datenübertragbarkeit (Art. 15 und 20 DSGVO; WP 248 Rev.01, 21 und 28)	Das Recht auf Auskunft kann elektronisch oder postalisch gegenüber der Gesundheitsminister:in wahrgenommen werden. Die nähere Modalitäten zur Ausübung des Rechts auf Auskunft sind in der noch zur Verfügung zu stellenden Datenschutzerklärung zu beschreiben. Das Recht auf Datenübertragbarkeit steht gemäß Art. 20 Abs. 1 Buchstabe a DSGVO nicht zu, weil die Verarbeitung ▪ 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 Mitgliedstaates, nämlich des Bundesgesetzes über die Dokumentation im Gesundheitswesen erfolgt. **Die Anforderung "Bewertung des Auskunftsrechts der betroffenen Personen und ihres Rechts auf Datenübertragbarkeit" ist aufgrund der grundsätzlichen Umsetzbarkeit als erfüllbar anzusehen.**
Recht auf Berichtigung und Löschung (Art. 16, 17 und 19, WP 248 Rev.01, 21 und 28)	Das Recht auf Berichtigung kann elektronisch oder postalisch gegenüber der Gesundheitsminister:in wahrgenommen werden. Die nähere Modalitäten zur Ausübung des Rechts auf Berichtigung sind in der noch zur Verfügung zu stellenden Datenschutzerklärung zu beschreiben. 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 Gesundheitsminister:in als Verantwortliche unterliegt, erforderlich ist. Die *rechtlichen Verpflichtungen nach dem Recht eines Mitgliedstaats* sind in diesem Fall die verfassungsrechtlichen Bestimmungen zur Ministerverantwortlichkeit, wie insbesondere Art. 76 B-VG, sowie die Bestimmungen des Bundesgesetzes über die Dokumentation im Gesundheitswesen. **Die Anforderung "Bewertung des Rechts auf Berichtigung und Lö-**

	schung" ist aufgrund der grundsätzlichen Umsetzbarkeit als erfüllbar anzusehen.
Widerspruchsrecht und Recht auf Einschränkung der Verarbeitung (Art. 18, 19 und 21; WP 248 Rev.01, 21 und 28)	Das Recht auf Einschränkung der Verarbeitung ist gegenüber der Gesundheitsminister:in wahrzunehmen. Die nähere Modalitäten zur Ausübung des Rechts auf Einschränkung der Verarbeitung sind in der noch zur Verfügung zu stellenden Datenschutzerklärung zu beschreiben. Das Widerspruchsrecht steht nicht zu, weil die Verarbeitung weder aufgrund öffentlicher Interessen (Art. 6 Abs. 1 Buchstabe e DSGVO) noch aufgrund berechtigter Interessen (Art. 6 Abs. 1 Buchstabe f DSGVO) noch zu Zwecken der Direktwerbung erfolgt. Die Verarbeitung erfolgt 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 Verarbeitungstätigkeit „DIAG" wohl der Fall wäre – erfolgt. **Die Anforderung "Bewertung des Widerspruchsrechts und des Rechts auf Einschränkung der Verarbeitung" ist aufgrund der grundsätzlichen Umsetzbarkeit als erfüllbar anzusehen.**
Verhältnis zu Auftragsverarbeitern (Art. 28 DSGVO; WP 248 Rev.01, 21 und 28)	Als Auftragsverarbeiter:in ist gesetzlich der Dachverband der österreichischen Sozialversicherungsträger vorgesehen (§ 5a und § 6c des Bundesgesetzes über die Dokumentation im Gesundheitswesen). Hierbei 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 Bundesgesetz über die Dokumentation im Gesundheitswesen oder in einer darauf basierenden Verordnung gibt, die die Anforderungen des Art. 28 Abs. 3 DSGVO erfüllt, sind Auftragsverarbeitungsvereinbarungen abzuschließen. § 5a und § 6c des Bundesgesetzes über die Dokumentation im Gesundheitswesen regeln nur die Aufgaben des Dachverbands der österreichischen Sozialversicherungsträger, aber nicht die gemäß erforderlichen Bestimmungen von Auftragsverarbeitungsvereinbarungen. Der Abschluss der Auftragsverarbeitungsvereinbarungen hat gemäß Art. 28 Abs. 9 DSGVO schriftlich zu erfolgen. **Die Anforderung "Bewertung des Verhältnisses zu Auftragsverarbeiterinnen und Auftragsverarbeitern" ist aufgrund der grundsätzlichen Umsetzbarkeit als erfüllbar anzusehen.**
Schutzmaßnahmen bei der Übermittlung in Drittländer (Kapitel V DSGVO; WP 248 Rev.01, 21 und 28)	Eine Übermittlung in Drittländer ist nicht vorgesehen. Es sind daher keine spezifischen Schutzmaßnahmen für die Übermittlung in Drittländer vorgesehen. **Die Anforderung "Bewertung der Schutzmaßnahmen bei der Übermittlung in Drittländer" ist aufgrund der nicht vorgesehenen Übermittlung in Drittländer als erfüllt anzusehen.**
Vorherige Konsultation (Art. 36 und EG 96 DSGVO; WP 248 Rev.01, 21 und 28)	Die vorherige Konsultation der Datenschutzbehörde ist nicht erforderlich, weil die Verantwortlichen folgende Maßnahmen zur Eindämmung der Risiken treffen: ▪ die Beschränkung des Zugriffs auf Mitarbeiter:innen des Gesundheitsministeriums (§ 4 Abs. 3 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ die Verschwiegenheitspflicht für alle an der Verarbeitung beteiligten Personen und zwar auch nach Beendigung ihrer Tätigkeit (§ 4 Abs. 3 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ der Zugriff auf Rohdaten und Pseudonyme darf nur insoweit erteilt werden,

	als dies eine wesentliche Voraussetzung zur Wahrnehmung einer gesetzlich übertragenen Aufgabe ist (§ 4 Abs. 3 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ der Ausschluss des Zugriffs für Analyist:innen auf Rohdaten und Pseudonyme (§ 4 Abs. 3 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ die Pflicht zur Einhaltung der Datenverarbeitungsgrundsätze gemäß Art. 5 DSGVO (§ 4 Abs. 3 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ die Pflicht zur Löschung von bereichsspezifischen Personenkennzeichen und sonstigen Pseudonymen nach 15 Jahren (§ 4 Abs. 5 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ die Pflicht zur Löschung der übrigen Daten nach 25 Jahren (§ 4 Abs. 5 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ die Pflicht zur Einhaltung der Löschfristen gemäß § 4 Abs. 5 des Bundesgesetzes über die Dokumentation im Gesundheitswesen auch für die Bundesanstalt „Statistik Österreich“ (§ 5 Abs. 1 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ die Pflicht zur Einhaltung der Löschfristen gemäß § 4 Abs. 5 des Bundesgesetzes über die Dokumentation im Gesundheitswesen auch für sonstige Empfänger:innen (§ 5 Abs. 4 und § 6e Abs. 3 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ Pseudonymisierung durch die Pseudonymisierungsstelle des Dachverbands der österreichischen Sozialversicherungsträger (§ 5a des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ die Pflicht des ambulanten Bereichs spätestens ab 1. Jänner 2025 gemäß § 6 Abs. 1 des Bundesgesetzes über die Dokumentation im Gesundheitswesen zu codieren; ▪ sämtliche Datenübermittlungen haben verschlüsselt zu erfolgen (§ 5 Abs. 1 und § 9 Abs. 2 der Gesundheitsdokumentationsverordnung); ▪ Aufnahmezahlen sind durch nicht rückrechenbare Datensatz-IDs und Geburtsdaten durch Altersgruppen zu ersetzen (§ 6a Abs. 1 und § 6b des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ Verkettungsverbot für den Dachverband der österreichischen Sozialversicherungsträger hinsichtlich der im Hauptstück B geregelten Diagnosen- und Leistungsdokumentation im ambulanten Bereich (§ 6f Abs. 1 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ die Pflicht Vollständigkeits- und Plausibilitätsprüfungen durchzuführen (§ 7 der Gesundheitsdokumentationsverordnung); ▪ die Pflicht zur Verwendung des SHA-256-Algorithmus, der nach der aktuellen Technischen Richtlinie des BSI vom 9.1.2023 zu kryptographischen Verfahren: Empfehlungen und Schlüssellängen (BSI-TR-02102-1), 46 im Jahr 2023 auch noch als stark gilt (§ 8 der Gesundheitsdokumentationsverordnung); ▪ Dokumentation der Rechtsgrundlagen im Rechtsinformationssystem des Bundes (siehe unten Feld „ABHILFEMASSNAHMEN / Transparenz“); ▪ 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“). **Die Anforderung “Bewertung der vorherigen Konsultation” ist aufgrund der durchgeführten vorherigen Konsultation als erfüllbar anzusehen.**

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:

Physische, materielle oder	Ursache: Physische, materielle oder immaterielle Schäden können für die

immaterielle Schäden (EG 90 iVm 85 DSGVO; WP 248 Rev.01, 21 und 28)	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 das DIAG aufgedeckten Schäden. Art: Denkbar sind beispielsweise materielle oder immaterielle Schäden, die als Folge aufgedeckten Fehlverhaltens auftreten, wie etwa Verdienstentgang. Physische Schäden sind nicht zu erwarten, weil das DIAG keine unmittelbaren physischen Eingriffe nach sich ziehen. Besonderheit: Die Besonderheit des gegenständlichen Risikos für physische, materielle oder immaterielle Schäden ergibt sich aus der (theoretischen) Nachverfolgbarkeit der Arbeit von betroffenen Personen. Schwere: 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. Eintrittswahrscheinlichkeit: 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: ▪ die Beschränkung des Zugriffs auf Mitarbeiter:innen des Gesundheitsministeriums (§ 4 Abs. 3 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ die Verschwiegenheitspflicht für alle an der Verarbeitung beteiligten Personen und zwar auch nach Beendigung ihrer Tätigkeit (§ 4 Abs. 3 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ der Zugriff auf Rohdaten und Pseudonyme darf nur insoweit erteilt werden, als dies eine wesentliche Voraussetzung zur Wahrnehmung einer gesetzlich übertragenen Aufgabe ist (§ 4 Abs. 3 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ der Ausschluss des Zugriffs für Analyist:innen auf Rohdaten und Pseudonyme (§ 4 Abs. 3 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ die Pflicht zur Einhaltung der Datenverarbeitungsgrundsätze gemäß Art. 5 DSGVO (§ 4 Abs. 3 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ die Pflicht zur Löschung von bereichsspezifischen Personenkennzeichen und sonstigen Pseudonymen nach 15 Jahren (§ 4 Abs. 5 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ die Pflicht zur Löschung der übrigen Daten nach 25 Jahren (§ 4 Abs. 5 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ die Pflicht zur Einhaltung der Löschfristen gemäß § 4 Abs. 5 des Bundesgesetzes über die Dokumentation im Gesundheitswesen auch für die Bundesanstalt „Statistik Österreich“ (§ 5 Abs. 1 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ die Pflicht zur Einhaltung der Löschfristen gemäß § 4 Abs. 5 des Bundesgesetzes über die Dokumentation im Gesundheitswesen auch für sonstige Empfänger:innen (§ 5 Abs. 4 und § 6e Abs. 3 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ Pseudonymisierung durch die Pseudonymisierungsstelle des Dachverbands der österreichischen Sozialversicherungsträger (§ 5a des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ die Pflicht des ambulanten Bereichs spätestens ab 1. Jänner 2025 gemäß § 6 Abs. 1 des Bundesgesetzes über die Dokumentation im Gesundheitswesen zu codieren;

	▪ sämtliche Datenübermittlungen haben verschlüsselt zu erfolgen (§ 5 Abs. 1 und § 9 Abs. 2 der Gesundheitsdokumentationsverordnung); ▪ Aufnahmezahlen sind durch nicht rückrechenbare Datensatz-IDs und Geburtsdaten durch Altersgruppen zu ersetzen (§ 6a Abs. 1 und § 6b des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ Verkettungsverbot für den Dachverband der österreichischen Sozialversicherungsträger hinsichtlich der im Hauptstück B geregelten Diagnosen- und Leistungsdokumentation im ambulanten Bereich (§ 6f Abs. 1 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ die Pflicht Vollständigkeits- und Plausibilitätsprüfungen durchzuführen (§ 7 der Gesundheitsdokumentationsverordnung); ▪ die Pflicht zur Verwendung des SHA-256-Algorithmus, der nach der aktuellen Technischen Richtlinie des BSI vom 9.1.2023 zu kryptographischen Verfahren: Empfehlungen und Schlüssellängen (BSI-TR-02102-1), 46 im Jahr 2023 auch noch als stark gilt (§ 8 der Gesundheitsdokumentationsverordnung); ▪ die Heranziehung von ISO-27k zertifizierten (Sub-)Auftragsverarbeiter:innen; ▪ das für Beamt:innen bei der Verantwortlichen und den Empfänger:innen 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). **Aufgrund der gegenständlichen Verarbeitung, insbesondere der Heranziehung von ISO-27k zertifizierten (Sub-)Auftragsverarbeiter:innen sowie der geltenden, strengen Strafdrohungen ist nicht von einem substanziellen Risiko für das Auftreten physischer, materieller und immaterieller Schäden auszugehen, womit die gegenständliche Anforderung als erfüllt angesehen werden kann.**
Verlust der Kontrolle über personenbezogene Daten (EG 90 iVm 85 DSGVO; WP 248 Rev.01, 21 und 28)	Ursache: 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. Art: Beim Verlust der Kontrolle über personenbezogene Daten haben die betroffenen Personen keinerlei Möglichkeit auf die Verarbeitung Einfluss zu nehmen und sind ihrer Betroffenenrechte beraubt. Besonderheit: 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. Schwere: Von ihrer Schwere ist der Verlust der Kontrolle über personenbezogene Daten nicht von vergleichbaren Risiken aufgrund anderer gesetzlich vorgesehener Verarbeitungen zu unterscheiden. Eintrittswahrscheinlichkeit: 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: ▪ die Beschränkung des Zugriffs auf Mitarbeiter:innen des Gesundheitsministeriums (§ 4 Abs. 3 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ die Verschwiegenheitspflicht für alle an der Verarbeitung beteiligten Personen und zwar auch nach Beendigung ihrer Tätigkeit (§ 4 Abs. 3 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ der Zugriff auf Rohdaten und Pseudonyme darf nur insoweit erteilt werden, als dies eine wesentliche Voraussetzung zur Wahrnehmung einer gesetzlich übertragenen Aufgabe ist (§ 4 Abs. 3 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ der Ausschluss des Zugriffs für Analyst:innen auf Rohdaten und Pseudonyme (§ 4 Abs. 3 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ die Pflicht zur Einhaltung der Datenverarbeitungsgrundsätze gemäß Art. 5 DSGVO (§ 4 Abs. 3 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ die Pflicht zur Löschung von bereichsspezifischen Personenkennzeichen und sonstigen Pseudonymen nach 15 Jahren (§ 4 Abs. 5 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ die Pflicht zur Löschung der übrigen Daten nach 25 Jahren (§ 4 Abs. 5 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ die Pflicht zur Einhaltung der Löschfristen gemäß § 4 Abs. 5 des Bundesgesetzes über die Dokumentation im Gesundheitswesen auch für die Bundesanstalt „Statistik Österreich“ (§ 5 Abs. 1 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ die Pflicht zur Einhaltung der Löschfristen gemäß § 4 Abs. 5 des Bundesgesetzes über die Dokumentation im Gesundheitswesen auch für sonstige Empfänger:innen (§ 5 Abs. 4 und § 6e Abs. 3 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ Pseudonymisierung durch die Pseudonymisierungsstelle des Dachverbands der österreichischen Sozialversicherungsträger (§ 5a des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ die Pflicht des ambulanten Bereichs spätestens ab 1. Jänner 2025 gemäß § 6 Abs. 1 des Bundesgesetzes über die Dokumentation im Gesundheitswesen zu codieren; ▪ sämtliche Datenübermittlungen haben verschlüsselt zu erfolgen (§ 5 Abs. 1 und § 9 Abs. 2 der Gesundheitsdokumentationsverordnung); ▪ Aufnahmezahlen sind durch nicht rückrechenbare Datensatz-IDs und Geburtsdaten durch Altersgruppen zu ersetzen (§ 6a Abs. 1 und § 6b des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ Verkettungsverbot für den Dachverband der österreichischen Sozialversicherungsträger hinsichtlich der im Hauptstück B geregelten Diagnosen- und Leistungsdokumentation im ambulanten Bereich (§ 6f Abs. 1 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ die Pflicht Vollständigkeits- und Plausibilitätsprüfungen durchzuführen (§ 7 der Gesundheitsdokumentationsverordnung); ▪ die Pflicht zur Verwendung des SHA-256-Algorithmus, der nach der aktuellen Technischen Richtlinie des BSI vom 9.1.2023 zu kryptographischen Verfahren: Empfehlungen und Schlüssellängen (BSI-TR-02102-1), 46 im Jahr 2023 auch noch als stark gilt (§ 8 der Gesundheitsdokumentationsverordnung); ▪ die Heranziehung von ISO-27k zertifizierten (Sub-)Auftragsverarbeiter:innen; ▪ das für Beamt:innen bei der Verantwortlichen und den Empfänger:innen 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). **Aufgrund der gegenständlichen Verarbeitung, insbesondere der Heranziehung von ISO-27k zertifizierten (Sub-)Auftragsverarbeiter:innen sowie 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.**
Diskriminierung (EG 90 iVm 85 DSGVO; WP 248 Rev.01, 21 und 28)	Ursache: 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. Art: 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. Besonderheit: 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 der gesetzlich festgelegte Auftragsverarbeiter für das DIAG (siehe oben Feld „BEWERTUNG / Auftragsverarbeiter:innen“). Schwere: Diskrimierungen sind theoretisch denkbar; rechtlich vorgesehene Sanktionen sind allerdings nicht als rechtlich verwerfliche Diskriminierungen anzusehen. Eintrittswahrscheinlichkeit: 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: ▪ die Beschränkung des Zugriffs auf Mitarbeiter:innen des Gesundheitsministeriums (§ 4 Abs. 3 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ die Verschwiegenheitspflicht für alle an der Verarbeitung beteiligten Personen und zwar auch nach Beendigung ihrer Tätigkeit (§ 4 Abs. 3 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ der Zugriff auf Rohdaten und Pseudonyme darf nur insoweit erteilt werden, als dies eine wesentliche Voraussetzung zur Wahrnehmung einer gesetzlich übertragenen Aufgabe ist (§ 4 Abs. 3 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ der Ausschluss des Zugriffs für Analyist:innen auf Rohdaten und Pseudonyme (§ 4 Abs. 3 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ die Pflicht zur Einhaltung der Datenverarbeitungsgrundsätze gemäß Art. 5 DSGVO (§ 4 Abs. 3 des Bundesgesetzes über die Dokumentation im

	Gesundheitswesen); ▪ die Pflicht zur Löschung von bereichsspezifischen Personenkennzeichen und sonstigen Pseudonymen nach 15 Jahren (§ 4 Abs. 5 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ die Pflicht zur Löschung der übrigen Daten nach 25 Jahren (§ 4 Abs. 5 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ die Pflicht zur Einhaltung der Löschfristen gemäß § 4 Abs. 5 des Bundesgesetzes über die Dokumentation im Gesundheitswesen auch für die Bundesanstalt „Statistik Österreich“ (§ 5 Abs. 1 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ die Pflicht zur Einhaltung der Löschfristen gemäß § 4 Abs. 5 des Bundesgesetzes über die Dokumentation im Gesundheitswesen auch für sonstige Empfänger:innen (§ 5 Abs. 4 und § 6e Abs. 3 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ Pseudonymisierung durch die Pseudonymisierungsstelle des Dachverbands der österreichischen Sozialversicherungsträger (§ 5a des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ die Pflicht des ambulanten Bereichs spätestens ab 1. Jänner 2025 gemäß § 6 Abs. 1 des Bundesgesetzes über die Dokumentation im Gesundheitswesen zu codieren; ▪ sämtliche Datenübermittlungen haben verschlüsselt zu erfolgen (§ 5 Abs. 1 und § 9 Abs. 2 der Gesundheitsdokumentationsverordnung); ▪ Aufnahmezahlen sind durch nicht rückrechenbare Datensatz-IDs und Geburtsdaten durch Altersgruppen zu ersetzen (§ 6a Abs. 1 und § 6b des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ Verkettungsverbot für den Dachverband der österreichischen Sozialversicherungsträger hinsichtlich der im Hauptstück B geregelten Diagnosen- und Leistungsdokumentation im ambulanten Bereich (§ 6f Abs. 1 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ die Pflicht Vollständigkeits- und Plausibilitätsprüfungen durchzuführen (§ 7 der Gesundheitsdokumentationsverordnung); ▪ die Pflicht zur Verwendung des SHA-256-Algorithmus, der nach der aktuellen Technischen Richtlinie des BSI vom 9.1.2023 zu kryptographischen Verfahren: Empfehlungen und Schlüssellängen (BSI-TR-02102-1), 46 im Jahr 2023 auch noch als stark gilt (§ 8 der Gesundheitsdokumentationsverordnung); ▪ die Heranziehung von ISO-27k zertifizierten (Sub-)Auftragsverarbeiter:innen; ▪ das für Beamt:innen bei der Verantwortlichen und den Empfänger:innen 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). **Aufgrund der gegenständlichen Verarbeitung, insbesondere der Heranziehung von ISO-27k zertifizierten (Sub-)Auftragsverarbeiter:innen sowie 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.**
Identitätsdiebstahl oder -betrug (EG 90 iVm 85 DSGVO; WP 248 Rev.01, 21 und 28)	Ursache: 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. Art: 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. Besonderheit: Die Besonderheit des gegenständlichen Risikos für Identitätsdiebstahl oder -betrug ergibt sich vor allem aus der gesetzlichen Regelung, die dem DIAG zugrunde liegt. Dass weder Passwörter noch Nutzerkennungen oder Kreditkarteninformationen verarbeitet werden, senkt das Risiko für Identitätsdiebstahl oder -betrug. Schwere: Identitätsdiebstahl oder -betrug können – wie bereits ausgeführt – zu hohen, finanziellen Schäden bei den betroffenen Personen führen. Eintrittswahrscheinlichkeit: 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. Auch durch die folgenden bereits im Entwurf bzw. geltenden Recht enthaltenen technischen und organisatorischen Maßnahmen soll die Sicherheit der Verarbeitung erhöht und das Risiko für Identitätsdiebstahl oder -betrug gesenkt werden: ▪ die Beschränkung des Zugriffs auf Mitarbeiter:innen des Gesundheitsministeriums (§ 4 Abs. 3 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ die Verschwiegenheitspflicht für alle an der Verarbeitung beteiligten Personen und zwar auch nach Beendigung ihrer Tätigkeit (§ 4 Abs. 3 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ der Zugriff auf Rohdaten und Pseudonyme darf nur insoweit erteilt werden, als dies eine wesentliche Voraussetzung zur Wahrnehmung einer gesetzlich übertragenen Aufgabe ist (§ 4 Abs. 3 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ der Ausschluss des Zugriffs für Analyist:innen auf Rohdaten und Pseudonyme (§ 4 Abs. 3 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ die Pflicht zur Einhaltung der Datenverarbeitungsgrundsätze gemäß Art. 5 DSGVO (§ 4 Abs. 3 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ die Pflicht zur Löschung von bereichsspezifischen Personenkennzeichen und sonstigen Pseudonymen nach 15 Jahren (§ 4 Abs. 5 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ die Pflicht zur Löschung der übrigen Daten nach 25 Jahren (§ 4 Abs. 5 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ die Pflicht zur Einhaltung der Löschfristen gemäß § 4 Abs. 5 des Bundesgesetzes über die Dokumentation im Gesundheitswesen auch für die Bundesanstalt „Statistik Österreich“ (§ 5 Abs. 1 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ die Pflicht zur Einhaltung der Löschfristen gemäß § 4 Abs. 5 des Bundesgesetzes über die Dokumentation im Gesundheitswesen auch für sonstige Empfänger:innen (§ 5 Abs. 4 und § 6e Abs. 3 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ Pseudonymisierung durch die Pseudonymisierungsstelle des Dachverbands der österreichischen Sozialversicherungsträger (§ 5a des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ die Pflicht des ambulanten Bereichs spätestens ab 1. Jänner 2025 gemäß § 6 Abs. 1 des Bundesgesetzes über die Dokumentation im Gesundheitswesen zu codieren; ▪ sämtliche Datenübermittlungen haben verschlüsselt zu erfolgen (§ 5 Abs. 1 und § 9 Abs. 2 der Gesundheitsdokumentationsverordnung); ▪ Aufnahmezahlen sind durch nicht rückrechenbare Datensatz-IDs und Geburtsdaten durch Altersgruppen zu ersetzen (§ 6a Abs. 1 und § 6b des Bundesgesetzes über die Dokumentation im Gesundheitswesen);

	▪ Verkettungsverbot für den Dachverband der österreichischen Sozialversicherungsträger hinsichtlich der im Hauptstück B geregelten Diagnosen- und Leistungsdokumentation im ambulanten Bereich (§ 6f Abs. 1 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ die Pflicht Vollständigkeits- und Plausibilitätsprüfungen durchzuführen (§ 7 der Gesundheitsdokumentationsverordnung); ▪ die Pflicht zur Verwendung des SHA-256-Algorithmus, der nach der aktuellen Technischen Richtlinie des BSI vom 9.1.2023 zu kryptographischen Verfahren: Empfehlungen und Schlüssellängen (BSI-TR-02102-1), 46 im Jahr 2023 auch noch als stark gilt (§ 8 der Gesundheitsdokumentationsverordnung); ▪ die Heranziehung von ISO-27k zertifizierten (Sub-)Auftragsverarbeiter:innen; ▪ das für Beamt:innen bei der Verantwortlichen und den Empfänger:innen 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). **Aufgrund der gegenständlichen Verarbeitung, insbesondere der Heranziehung von ISO-27k zertifizierten (Sub-)Auftragsverarbeiter:innen sowie der geltenden, strengen Strafdrohungen ist nicht von einem substanziellen Risiko für Identitätsdiebstahl oder -betrug auszugehen, womit die gegenständliche Anforderung als erfüllt angesehen werden kann.**
Finanzielle Verluste (EG 90 iVm 85 DSGVO; WP 248 Rev.01, 21 und 28)	Ursache: 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. Art: Finanzielle Verluste sind geldwerte Schäden und können insbesondere im Entgang von Verdienstmöglichkeiten liegen. Besonderheit: Die Besonderheit des gegenständlichen Risikos für finanzielle Verluste ergibt sich vor allem aus der gesetzlichen Regelung, die dem DIAG zugrunde liegt. Dass weder Passwörter noch Nutzerkennungen noch Kreditkarteninformationen verarbeitet werden, senkt das Risiko für finanzielle Verluste aufgrund von Identitätsdiebstahl oder -betrug. Schwere: Identitätsdiebstahl oder -betrug können – wie bereits oben ausgeführt – zu hohen, finanziellen Schäden bei den betroffenen Personen führen. Eintrittswahrscheinlichkeit: 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: ▪ die Beschränkung des Zugriffs auf Mitarbeiter:innen des Gesundheitsministeriums (§ 4 Abs. 3 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ die Verschwiegenheitspflicht für alle an der Verarbeitung beteiligten Personen und zwar auch nach Beendigung ihrer Tätigkeit (§ 4 Abs. 3 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ der Zugriff auf Rohdaten und Pseudonyme darf nur insoweit erteilt werden,

	als dies eine wesentliche Voraussetzung zur Wahrnehmung einer gesetzlich übertragenen Aufgabe ist (§ 4 Abs. 3 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ der Ausschluss des Zugriffs für Analyist:innen auf Rohdaten und Pseudonyme (§ 4 Abs. 3 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ die Pflicht zur Einhaltung der Datenverarbeitungsgrundsätze gemäß Art. 5 DSGVO (§ 4 Abs. 3 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ die Pflicht zur Löschung von bereichsspezifischen Personenkennzeichen und sonstigen Pseudonymen nach 15 Jahren (§ 4 Abs. 5 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ die Pflicht zur Löschung der übrigen Daten nach 25 Jahren (§ 4 Abs. 5 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ die Pflicht zur Einhaltung der Löschfristen gemäß § 4 Abs. 5 des Bundesgesetzes über die Dokumentation im Gesundheitswesen auch für die Bundesanstalt „Statistik Österreich“ (§ 5 Abs. 1 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ die Pflicht zur Einhaltung der Löschfristen gemäß § 4 Abs. 5 des Bundesgesetzes über die Dokumentation im Gesundheitswesen auch für sonstige Empfänger:innen (§ 5 Abs. 4 und § 6e Abs. 3 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ Pseudonymisierung durch die Pseudonymisierungsstelle des Dachverbands der österreichischen Sozialversicherungsträger (§ 5a des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ die Pflicht des ambulanten Bereichs spätestens ab 1. Jänner 2025 gemäß § 6 Abs. 1 des Bundesgesetzes über die Dokumentation im Gesundheitswesen zu codieren; ▪ sämtliche Datenübermittlungen haben verschlüsselt zu erfolgen (§ 5 Abs. 1 und § 9 Abs. 2 der Gesundheitsdokumentationsverordnung); ▪ Aufnahmezahlen sind durch nicht rückrechenbare Datensatz-IDs und Geburtsdaten durch Altersgruppen zu ersetzen (§ 6a Abs. 1 und § 6b des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ Verkettungsverbot für den Dachverband der österreichischen Sozialversicherungsträger hinsichtlich der im Hauptstück B geregelten Diagnosen- und Leistungsdokumentation im ambulanten Bereich (§ 6f Abs. 1 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ die Pflicht Vollständigkeits- und Plausibilitätsprüfungen durchzuführen (§ 7 der Gesundheitsdokumentationsverordnung); ▪ die Pflicht zur Verwendung des SHA-256-Algorithmus, der nach der aktuellen Technischen Richtlinie des BSI vom 9.1.2023 zu kryptographischen Verfahren: Empfehlungen und Schlüssellängen (BSI-TR-02102-1), 46 im Jahr 2023 auch noch als stark gilt (§ 8 der Gesundheitsdokumentationsverordnung); ▪ die Heranziehung von ISO-27k zertifizierten (Sub-)Auftragsverarbeiter:innen; ▪ das für Beamt:innen bei der Verantwortlichen und den Empfänger:innen 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). **Aufgrund der gegenständlichen Verarbeitung, insbesondere der Heranziehung von ISO-27k zertifizierten (Sub-)Auftragsverarbeiter:innen sowie der geltenden, strengen Strafdrohungen ist nicht von finanziellen Verlusten für die betroffenen Personen auszugehen, womit die gegenständliche Anforderung als erfüllt angesehen werden kann.**

Unbefugte Aufhebung der Pseudonymisierung (EG 90 iVm 85 DSGVO; WP 248 Rev.01, 21 und 28)	Ursache: Die unbefugte Aufhebung der Pseudonymisierung geschieht typischerweise durch Verkettung grundsätzlich pseudonymisierter Datensätze. Art: Die unbefugte Aufhebung der Pseudonymisierung kann andere Risiken, wie etwa finanzielle Verluste oder Nachteile aus Diskriminierung zur Folge haben. Besonderheit: Die Besonderheit des gegenständlichen Risikos ergibt sich aus der gesetzlichen Regelung, die von vornherein bestenfalls die Verarbeitung pseudonymisierter Daten, wenn nicht sogar nur anonymisierter Daten vorsieht. Schwere: Die Schwere des Risikos ergibt sich vor allem aus den anschließenden Risiken, wie etwa finanziellen Verlusten oder Nachteilen aus Diskriminierung. Eintrittswahrscheinlichkeit: 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: ▪ die Beschränkung des Zugriffs auf Mitarbeiter:innen des Gesundheitsministeriums (§ 4 Abs. 3 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ die Verschwiegenheitspflicht für alle an der Verarbeitung beteiligten Personen und zwar auch nach Beendigung ihrer Tätigkeit (§ 4 Abs. 3 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ der Zugriff auf Rohdaten und Pseudonyme darf nur insoweit erteilt werden, als dies eine wesentliche Voraussetzung zur Wahrnehmung einer gesetzlich übertragenen Aufgabe ist (§ 4 Abs. 3 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ der Ausschluss des Zugriffs für Analyist:innen auf Rohdaten und Pseudonyme (§ 4 Abs. 3 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ die Pflicht zur Einhaltung der Datenverarbeitungsgrundsätze gemäß Art. 5 DSGVO (§ 4 Abs. 3 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ die Pflicht zur Löschung von bereichsspezifischen Personenkennzeichen und sonstigen Pseudonymen nach 15 Jahren (§ 4 Abs. 5 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ die Pflicht zur Löschung der übrigen Daten nach 25 Jahren (§ 4 Abs. 5 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ die Pflicht zur Einhaltung der Löschfristen gemäß § 4 Abs. 5 des Bundesgesetzes über die Dokumentation im Gesundheitswesen auch für die Bundesanstalt „Statistik Österreich“ (§ 5 Abs. 1 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ die Pflicht zur Einhaltung der Löschfristen gemäß § 4 Abs. 5 des Bundesgesetzes über die Dokumentation im Gesundheitswesen auch für sonstige Empfänger:innen (§ 5 Abs. 4 und § 6e Abs. 3 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ Pseudonymisierung durch die Pseudonymisierungsstelle des Dachverbands der österreichischen Sozialversicherungsträger (§ 5a des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ die Pflicht des ambulanten Bereichs spätestens ab 1. Jänner 2025 gemäß § 6 Abs. 1 des Bundesgesetzes über die Dokumentation im Gesundheitswesen zu codieren; ▪ sämtliche Datenübermittlungen haben verschlüsselt zu erfolgen (§ 5 Abs. 1 und § 9 Abs. 2 der Gesundheitsdokumentationsverordnung); ▪ Aufnahmezahlen sind durch nicht rückrechenbare Datensatz-IDs und Geburtsdaten durch Altersgruppen zu ersetzen (§ 6a Abs. 1 und § 6b des Bundesgesetzes über die Dokumentation im Gesundheitswesen);

	▪ Verkettungsverbot für den Dachverband der österreichischen Sozialversicherungsträger hinsichtlich der im Hauptstück B geregelten Diagnosen- und Leistungsdokumentation im ambulanten Bereich (§ 6f Abs. 1 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ die Pflicht Vollständigkeits- und Plausibilitätsprüfungen durchzuführen (§ 7 der Gesundheitsdokumentationsverordnung); ▪ die Pflicht zur Verwendung des SHA-256-Algorithmus, der nach der aktuellen Technischen Richtlinie des BSI vom 9.1.2023 zu kryptographischen Verfahren: Empfehlungen und Schlüssellängen (BSI-TR-02102-1), 46 im Jahr 2023 auch noch als stark gilt (§ 8 der Gesundheitsdokumentationsverordnung); ▪ die Heranziehung von ISO-27k zertifizierten (Sub-)Auftragsverarbeiter:innen; ▪ das für Beamt:innen bei der Verantwortlichen und den Empfänger:innen 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). **Aufgrund der gegenständlichen Verarbeitung, insbesondere der Heranziehung von ISO-27k zertifizierten (Sub-)Auftragsverarbeiter:innen sowie 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.**
Rufschädigung (EG 90 iVm 85 DSGVO; WP 248 Rev.01, 21 und 28)	Ursache: Nachteile aus Rufschädigung sind theoretisch denkbar. Art: Nachteile aus Rufschädigung können sich infolge anderer Risiken, wie etwa Datenschutzverletzungen ergeben. Besonderheit: 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. Schwere: Die Schwere des Risikos kann theoretisch – je nach Art der potentiellen Rufschädigung – auch hoch sein. Eintrittswahrscheinlichkeit: 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: ▪ die Beschränkung des Zugriffs auf Mitarbeiter:innen des Gesundheitsministeriums (§ 4 Abs. 3 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ die Verschwiegenheitspflicht für alle an der Verarbeitung beteiligten Personen und zwar auch nach Beendigung ihrer Tätigkeit (§ 4 Abs. 3 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ der Zugriff auf Rohdaten und Pseudonyme darf nur insoweit erteilt werden, als dies eine wesentliche Voraussetzung zur Wahrnehmung einer gesetzlich übertragenen Aufgabe ist (§ 4 Abs. 3 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ der Ausschluss des Zugriffs für Analyist:innen auf Rohdaten und Pseudonyme (§ 4 Abs. 3 des Bundesgesetzes über die Dokumentation im Gesundheitswesen);

	▪ die Pflicht zur Einhaltung der Datenverarbeitungsgrundsätze gemäß Art. 5 DSGVO (§ 4 Abs. 3 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ die Pflicht zur Löschung von bereichsspezifischen Personenkennzeichen und sonstigen Pseudonymen nach 15 Jahren (§ 4 Abs. 5 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ die Pflicht zur Löschung der übrigen Daten nach 25 Jahren (§ 4 Abs. 5 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ die Pflicht zur Einhaltung der Löschfristen gemäß § 4 Abs. 5 des Bundesgesetzes über die Dokumentation im Gesundheitswesen auch für die Bundesanstalt „Statistik Österreich“ (§ 5 Abs. 1 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ die Pflicht zur Einhaltung der Löschfristen gemäß § 4 Abs. 5 des Bundesgesetzes über die Dokumentation im Gesundheitswesen auch für sonstige Empfänger:innen (§ 5 Abs. 4 und § 6e Abs. 3 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ Pseudonymisierung durch die Pseudonymisierungsstelle des Dachverbands der österreichischen Sozialversicherungsträger (§ 5a des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ die Pflicht des ambulanten Bereichs spätestens ab 1. Jänner 2025 gemäß § 6 Abs. 1 des Bundesgesetzes über die Dokumentation im Gesundheitswesen zu codieren; ▪ sämtliche Datenübermittlungen haben verschlüsselt zu erfolgen (§ 5 Abs. 1 und § 9 Abs. 2 der Gesundheitsdokumentationsverordnung); ▪ Aufnahmezahlen sind durch nicht rückrechenbare Datensatz-IDs und Geburtsdaten durch Altersgruppen zu ersetzen (§ 6a Abs. 1 und § 6b des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ Verkettungsverbot für den Dachverband der österreichischen Sozialversicherungsträger hinsichtlich der im Hauptstück B geregelten Diagnosen- und Leistungsdokumentation im ambulanten Bereich (§ 6f Abs. 1 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ die Pflicht Vollständigkeits- und Plausibilitätsprüfungen durchzuführen (§ 7 der Gesundheitsdokumentationsverordnung); ▪ die Pflicht zur Verwendung des SHA-256-Algorithmus, der nach der aktuellen Technischen Richtlinie des BSI vom 9.1.2023 zu kryptographischen Verfahren: Empfehlungen und Schlüssellängen (BSI-TR-02102-1), 46 im Jahr 2023 auch noch als stark gilt (§ 8 der Gesundheitsdokumentationsverordnung); ▪ die Heranziehung von ISO-27k zertifizierten (Sub-)Auftragsverarbeiter:innen; ▪ das für Beamt:innen bei der Verantwortlichen und den Empfänger:innen 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). **Aufgrund der gegenständlichen Verarbeitung, insbesondere der Heranziehung von ISO-27k zertifizierten (Sub-)Auftragsverarbeiter:innen sowie der geltenden, strengen Strafdrohungen ist nicht von einer Rufschädigung für betroffene Personen auszugehen, womit die gegenständliche Anforderung als erfüllt angesehen werden kann.**
Verlust der Vertraulichkeit bei Berufsgeheimnissen (EG 90 iVm 85 DSGVO; WP 248 Rev.01, 21 und 28)	Ursache: Der Verlust der Vertraulichkeit bei Berufsgeheimnissen ist theoretisch denkbar, wenn es zu Offenlegung durch Personen, die etwa dem Amtsgeheimnis unterliegen, kommt. Art: Der Verlust der Vertraulichkeit bei Berufsgeheimnissen kann andere

	Risiken, wie etwa finanzielle Verluste oder Nachteile aus Diskriminierung zur Folge haben. Besonderheit: Die Besonderheit des gegenständlichen Risikos ergibt sich vor allem daraus, dass die Verarbeitung nur durch Personen erfolgen darf, die einem Berufsgeheimnis (gemäß § 4 Abs. 3 des Bundesgesetzes über die Dokumentation im Gesundheitswesen) unterliegen. Schwere: Die Schwere des Risikos ergibt sich vor allem aus den anschließenden Risiken, wie etwa finanziellen Verlusten oder Nachteilen aus Diskriminierung. Eintrittswahrscheinlichkeit: 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: ▪ die Beschränkung des Zugriffs auf Mitarbeiter:innen des Gesundheitsministeriums (§ 4 Abs. 3 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ die Verschwiegenheitspflicht für alle an der Verarbeitung beteiligten Personen und zwar auch nach Beendigung ihrer Tätigkeit (§ 4 Abs. 3 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ der Zugriff auf Rohdaten und Pseudonyme darf nur insoweit erteilt werden, als dies eine wesentliche Voraussetzung zur Wahrnehmung einer gesetzlich übertragenen Aufgabe ist (§ 4 Abs. 3 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ der Ausschluss des Zugriffs für Analyist:innen auf Rohdaten und Pseudonyme (§ 4 Abs. 3 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ die Pflicht zur Einhaltung der Datenverarbeitungsgrundsätze gemäß Art. 5 DSGVO (§ 4 Abs. 3 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ die Pflicht zur Löschung von bereichsspezifischen Personenkennzeichen und sonstigen Pseudonymen nach 15 Jahren (§ 4 Abs. 5 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ die Pflicht zur Löschung der übrigen Daten nach 25 Jahren (§ 4 Abs. 5 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ die Pflicht zur Einhaltung der Löschfristen gemäß § 4 Abs. 5 des Bundesgesetzes über die Dokumentation im Gesundheitswesen auch für die Bundesanstalt „Statistik Österreich“ (§ 5 Abs. 1 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ die Pflicht zur Einhaltung der Löschfristen gemäß § 4 Abs. 5 des Bundesgesetzes über die Dokumentation im Gesundheitswesen auch für sonstige Empfänger:innen (§ 5 Abs. 4 und § 6e Abs. 3 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ Pseudonymisierung durch die Pseudonymisierungsstelle des Dachverbands der österreichischen Sozialversicherungsträger (§ 5a des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ die Pflicht des ambulanten Bereichs spätestens ab 1. Jänner 2025 gemäß § 6 Abs. 1 des Bundesgesetzes über die Dokumentation im Gesundheitswesen zu codieren; ▪ sämtliche Datenübermittlungen haben verschlüsselt zu erfolgen (§ 5 Abs. 1 und § 9 Abs. 2 der Gesundheitsdokumentationsverordnung); ▪ Aufnahmezahlen sind durch nicht rückrechenbare Datensatz-IDs und Geburtsdaten durch Altersgruppen zu ersetzen (§ 6a Abs. 1 und § 6b des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ Verkettungsverbot für den Dachverband der österreichischen Sozialversicherungsträger hinsichtlich der im Hauptstück B geregelten Diagnosen- und Leistungsdokumentation im ambulanten Bereich (§ 6f Abs. 1 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ die Pflicht Vollständigkeits- und Plausibilitätsprüfungen durchzuführen (§ 7

	der Gesundheitsdokumentationsverordnung); ▪ die Pflicht zur Verwendung des SHA-256-Algorithmus, der nach der aktuellen Technischen Richtlinie des BSI vom 9.1.2023 zu kryptographischen Verfahren: Empfehlungen und Schlüssellängen (BSI-TR-02102-1), 46 im Jahr 2023 auch noch als stark gilt (§ 8 der Gesundheitsdokumentationsverordnung); ▪ die Heranziehung von ISO-27k zertifizierten (Sub-)Auftragsverarbeiter:innen; ▪ das für Beamt:innen bei der Verantwortlichen und den Empfänger:innen 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). **Aufgrund der gegenständlichen Verarbeitung, insbesondere der Heranziehung von ISO-27k zertifizierten (Sub-)Auftragsverarbeiter:innen sowie der geltenden, strengen Strafdrohungen ist nicht von einem Verlust der Vertraulichkeit bei Berufsgeheimnissen auszugehen, womit die gegenständliche Anforderung als erfüllt angesehen werden kann.**
Erhebliche wirtschaftliche oder gesellschaftliche Nachteile (EG 90 iVm 85 DSGVO; WP 248 Rev.01, 21 und 28)	Ursache: Erhebliche wirtschaftliche oder gesellschaftliche Nachteile sind für die betroffenen Personen kaum denkbar (siehe oben Feld „RISIKEN / Physische, materielle oder immaterielle Schäden“, Seite 17 bzw. Feld„RISIKEN / Diskriminierung“, Seite 21), insbesondere weil die Möglichkeiten für Identitätsdiebstahl oder -betrug begrenzt sind. Art: 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. Besonderheit: 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 der gesetzlich festgelegte Auftragsverarbeiter für das DIAG (siehe oben Feld „BEWERTUNG / Auftragsverarbeiter:innen“). Schwere: Erhebliche wirtschaftliche oder gesellschaftliche Nachteile können vor allem den Verlust von Vertragsverhältnissen zu Sozialversicherungsträgern oder strafrechtliche Konsequenzen umfassen. Eintrittswahrscheinlichkeit: 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: ▪ die Beschränkung des Zugriffs auf Mitarbeiter:innen des Gesundheitsministeriums (§ 4 Abs. 3 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ die Verschwiegenheitspflicht für alle an der Verarbeitung beteiligten Personen und zwar auch nach Beendigung ihrer Tätigkeit (§ 4 Abs. 3 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ der Zugriff auf Rohdaten und Pseudonyme darf nur insoweit erteilt werden, als dies eine wesentliche Voraussetzung zur Wahrnehmung einer gesetzlich übertragenen Aufgabe ist (§ 4 Abs. 3 des Bundesgesetzes über die Dokumentation im Gesundheitswesen);

	▪ der Ausschluss des Zugriffs für Analyst:innen auf Rohdaten und Pseudonyme (§ 4 Abs. 3 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ die Pflicht zur Einhaltung der Datenverarbeitungsgrundsätze gemäß Art. 5 DSGVO (§ 4 Abs. 3 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ die Pflicht zur Löschung von bereichsspezifischen Personenkennzeichen und sonstigen Pseudonymen nach 15 Jahren (§ 4 Abs. 5 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ die Pflicht zur Löschung der übrigen Daten nach 25 Jahren (§ 4 Abs. 5 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ die Pflicht zur Einhaltung der Löschfristen gemäß § 4 Abs. 5 des Bundesgesetzes über die Dokumentation im Gesundheitswesen auch für die Bundesanstalt „Statistik Österreich“ (§ 5 Abs. 1 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ die Pflicht zur Einhaltung der Löschfristen gemäß § 4 Abs. 5 des Bundesgesetzes über die Dokumentation im Gesundheitswesen auch für sonstige Empfänger:innen (§ 5 Abs. 4 und § 6e Abs. 3 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ Pseudonymisierung durch die Pseudonymisierungsstelle des Dachverbands der österreichischen Sozialversicherungsträger (§ 5a des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ die Pflicht des ambulanten Bereichs spätestens ab 1. Jänner 2025 gemäß § 6 Abs. 1 des Bundesgesetzes über die Dokumentation im Gesundheitswesen zu codieren; ▪ sämtliche Datenübermittlungen haben verschlüsselt zu erfolgen (§ 5 Abs. 1 und § 9 Abs. 2 der Gesundheitsdokumentationsverordnung); ▪ Aufnahmezahlen sind durch nicht rückrechenbare Datensatz-IDs und Geburtsdaten durch Altersgruppen zu ersetzen (§ 6a Abs. 1 und § 6b des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ Verkettungsverbot für den Dachverband der österreichischen Sozialversicherungsträger hinsichtlich der im Hauptstück B geregelten Diagnosen- und Leistungsdokumentation im ambulanten Bereich (§ 6f Abs. 1 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ die Pflicht Vollständigkeits- und Plausibilitätsprüfungen durchzuführen (§ 7 der Gesundheitsdokumentationsverordnung); ▪ die Pflicht zur Verwendung des SHA-256-Algorithmus, der nach der aktuellen Technischen Richtlinie des BSI vom 9.1.2023 zu kryptographischen Verfahren: Empfehlungen und Schlüssellängen (BSI-TR-02102-1), 46 im Jahr 2023 auch noch als stark gilt (§ 8 der Gesundheitsdokumentationsverordnung); ▪ die Heranziehung von ISO-27k zertifizierten (Sub-)Auftragsverarbeiter:innen; ▪ das für Beamt:innen bei der Verantwortlichen und den Empfänger:innen 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). **Aufgrund der gegenständlichen Verarbeitung, insbesondere der Heranziehung von ISO-27k zertifizierten (Sub-)Auftragsverarbeiter:innen sowie 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.**
Nachteile durch	Ursache: Sollte die Verarbeitung unterbleiben, sind physische Nachteile für

Unterbleiben der Verarbeitung (EG 90 iVm 85 DSGVO; WP 248 Rev.01, 21 und 28)	die betroffenen Personen denkbar, weil die Gesundheitsversorgung möglicherweise nicht so gut funktioniert, wie sie funktionieren könnte. Art: 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 Erkankungen, 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. Besonderheit: 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 vor allem auf die Verbesserung der Gesundheitspolitik und Systemsteuerung abzielen. Eine Besonderheit der Verarbeitung besteht vor allem in ihren potentiell weiten Auswirkungen auf die Gesellschaft (vgl. in diesem Zusammenhang die bereits oben zitierten Forderungen nach verknüpfbaren, d.h. pseudonymisierten Gesundheitsdaten für Steuerungszwecke in: *Rechnungshof*, Gesundheitsdaten zur Pandemiebewältigung im ersten Jahr der COVID-19-Pandemie, Reihe BUND 2021/43, TZ 19.2 – ähnlich auch: *Panteli et al*, Health and Care Data – Approaches to data linkage for evidence-informed policy). Schwere: Im schlimmsten Fall können verzögerte Behandlungen bzw. nicht rechtzeitig erkannte Erkrankungen zu schwereren Verläufen oder sogar 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. Eintrittswahrscheinlichkeit: 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. **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 und vor allem so wie dies in der aktuell vorgeschlagenen Fassung des Bundesgesetzes über die Dokumentation im Gesundheitswesen vorgesehen ist.**

ABHILFEMASSNAHMEN
Als Maßnahmen, Garantien und Verfahren zur Eindämmung von Risiken werden insbesondere in den

Erwägungsgründen 28, 78 und 83 DSGVO genannt:	
Minimierung der Verarbeitung personenbezogener Daten (EG 78 und Art. 35 Abs. 7 Buchstabe d DSGVO; WP 248 Rev.01, 21 und 29)	Die Minimierung der Daten erfolgt insbesondere dadurch, dass ▪ die Zugriffe auf das DIAG auf Mitarbeiter:innen des Gesundheitsministeriums beschränkt sind (§ 4 Abs. 3 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ der Zugriff auf Rohdaten und Pseudonyme nur insoweit erteilt werden darf, als dies eine wesentliche Voraussetzung zur Wahrnehmung einer gesetzlich übertragenen Aufgabe ist (§ 4 Abs. 3 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ Analyst:innen vom Zugriff auf Rohdaten und Pseudonyme ausgeschlossen sind (§ 4 Abs. 3 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ bereichsspezifische Personenkennzeichen und sonstige Pseudonyme nach 15 Jahren zu löschen sind (§ 4 Abs. 5 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ alle übrigen Daten nach 25 Jahren zu löschen sind (§ 4 Abs. 5 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ die Pflicht zur Einhaltung der Löschfristen gemäß § 4 Abs. 5 des Bundesgesetzes über die Dokumentation im Gesundheitswesen auch für die Bundesanstalt „Statistik Österreich“ gilt (§ 5 Abs. 1 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ die Pflicht zur Einhaltung der Löschfristen gemäß § 4 Abs. 5 des Bundesgesetzes über die Dokumentation im Gesundheitswesen auch für sonstige Empfänger:innen gilt (§ 5 Abs. 4 und § 6e Abs. 3 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ eine Pseudonymisierung durch die Pseudonymisierungsstelle des Dachverbands der österreichischen Sozialversicherungsträger vorgenommen wird (§ 5a des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ der ambulante Bereichs spätestens ab 1. Jänner 2025 gemäß § 6 Abs. 1 des Bundesgesetzes über die Dokumentation im Gesundheitswesen zu codieren; ▪ Aufnahmezahlen durch nicht rückrechenbare Datensatz-IDs und Geburtsdaten durch Altersgruppen zu ersetzen sind (§ 6a Abs. 1 und § 6b des Bundesgesetzes über die Dokumentation im Gesundheitswesen). **Die Anforderung “Abhilfe durch Minimierung der Verarbeitung personenbezogener Daten” ist insbesondere aufgrund der Verwendung von bereichsspezifischen Personenkennzeichen als erfüllt anzusehen.**
Schnellstmögliche Pseudonymisierung personenbezogener Daten (EG 28 und 78 sowie Art. 35 Abs. 7 Buchstabe d DSGVO; WP 248 Rev.01, 21 und 29)	Mit einer Anonymisierung oder Aggregation ist ein hoher Informationsverlust verbunden (*Sachverständigenrat*, Rn 22). Dennoch sind die Regelungen des Bundesgesetzes über die Dokumentation im Gesundheitswesen nahe an der Anonymisierung, da sogar bestehende Pseudonyme zugriffsgeschützt sind (§ 4 Abs. 3 des Bundesgesetzes über die Dokumentation im Gesundheitswesen) und nach 15 Jahren zu löschen sind (§ 4 Abs. 5 des Bundesgesetzes über die Dokumentation im Gesundheitswesen). Da die Verarbeitung von Namen gar nicht vorgesehen ist, besteht grundsätzlich nur eine bestenfalls pseudonymisierte Verarbeitung. **Die Anforderung “Abhilfe durch schnellstmögliche Pseudonymisierung” ist aufgrund der Bestimmungen des Bundesgesetzes über die Dokumentation im Gesundheitswesen in der vorgeschlagenen Fassung als erfüllt anzusehen.**
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	Durch die Publikation des Bundesgesetzes über die Dokumentation im Gesundheitswesen 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.

und 29)	**Die Anforderung "Abhilfe durch Transparenz in Bezug auf die Funktionen und die Verarbeitung personenbezogener Daten" ist aufgrund der grundsätzlichen Machbarkeit der Veröffentlichung einer Datenschutzerklärung als erfüllbar anzusehen.**
Überwachung der Verarbeitung personenbezogener Daten durch die betroffenen Personen (EG 78 DSGVO und Art. 35 Abs. 7 Buchstabe d DSGVO; WP 248 Rev.01, 21 und 29)	Auf Grundlage der Datenschutz-Grundverordnung stehen natürlichen Personen folgende Rechte gegenüber der Verantwortlichen zu: ▪ das Recht auf Auskunft (Art. 15 DSGVO), ▪ das Recht auf Berichtigung (Art. 16 DSGVO) sowie ▪ das Recht auf Einschränkung der Verarbeitung (Art. 18 DSGVO). Diese Rechte können gegenüber der Verantwortlichen, d.h. der Gesundheitsminister:in, geltend gemacht werden. **Die Anforderung "Abhilfe durch Überwachung der Verarbeitung personenbezogener Daten durch die betroffenen Personen" ist aufgrund der grundsätzlichen Machbarkeit als erfüllbar anzusehen.**
Datensicherheitsmaßnahmen (EG 78 und 83 DSGVO sowie Art. 35 Abs. 7 Buchstabe d DSGVO; WP 248 Rev.01, 21 und 29)	Für die gegenständliche Verarbeitungstätigkeit sind insbesondere folgende Datensicherheitsmaßnahmen vorgesehen: ▪ die Beschränkung des Zugriffs auf Mitarbeiter:innen des Gesundheitsministeriums (§ 4 Abs. 3 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ die Verschwiegenheitspflicht für alle an der Verarbeitung beteiligten Personen und zwar auch nach Beendigung ihrer Tätigkeit (§ 4 Abs. 3 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ der Zugriff auf Rohdaten und Pseudonyme darf nur insoweit erteilt werden, als dies eine wesentliche Voraussetzung zur Wahrnehmung einer gesetzlich übertragenen Aufgabe ist (§ 4 Abs. 3 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ der Ausschluss des Zugriffs für Analyist:innen auf Rohdaten und Pseudonyme (§ 4 Abs. 3 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ die Pflicht zur Einhaltung der Datenverarbeitungsgrundsätze gemäß Art. 5 DSGVO (§ 4 Abs. 3 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ die Pflicht zur Löschung von bereichsspezifischen Personenkennzeichen und sonstigen Pseudonymen nach 15 Jahren (§ 4 Abs. 5 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ die Pflicht zur Löschung der übrigen Daten nach 25 Jahren (§ 4 Abs. 5 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ die Pflicht zur Einhaltung der Löschfristen gemäß § 4 Abs. 5 des Bundesgesetzes über die Dokumentation im Gesundheitswesen auch für die Bundesanstalt „Statistik Österreich" (§ 5 Abs. 1 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ die Pflicht zur Einhaltung der Löschfristen gemäß § 4 Abs. 5 des Bundesgesetzes über die Dokumentation im Gesundheitswesen auch für sonstige Empfänger:innen (§ 5 Abs. 4 und § 6e Abs. 3 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ Pseudonymisierung durch die Pseudonymisierungsstelle des Dachverbands der österreichischen Sozialversicherungsträger (§ 5a des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ die Pflicht des ambulanten Bereichs spätestens ab 1. Jänner 2025 gemäß § 6 Abs. 1 des Bundesgesetzes über die Dokumentation im Gesundheitswesen zu codieren; ▪ sämtliche Datenübermittlungen haben verschlüsselt zu erfolgen (§ 5 Abs. 1 und § 9 Abs. 2 der Gesundheitsdokumentationsverordnung); ▪ Aufnahmezahlen sind durch nicht rückrechenbare Datensatz-IDs und Geburtsdaten durch Altersgruppen zu ersetzen (§ 6a Abs. 1 und § 6b des Bundesgesetzes über die Dokumentation im Gesundheitswesen);

	▪ Verkettungsverbot für den Dachverband der österreichischen Sozialversicherungsträger hinsichtlich der im Hauptstück B geregelten Diagnosen- und Leistungsdokumentation im ambulanten Bereich (§ 6f Abs. 1 des Bundesgesetzes über die Dokumentation im Gesundheitswesen); ▪ die Pflicht Vollständigkeits- und Plausibilitätsprüfungen durchzuführen (§ 7 der Gesundheitsdokumentationsverordnung); ▪ die Pflicht zur Verwendung des SHA-256-Algorithmus, der nach der aktuellen Technischen Richtlinie des BSI vom 9.1.2023 zu kryptographischen Verfahren: Empfehlungen und Schlüssellängen (BSI-TR-02102-1), 46 im Jahr 2023 auch noch als stark gilt (§ 8 der Gesundheitsdokumentationsverordnung); ▪ die Heranziehung von ISO-27k zertifizierten (Sub-)Auftragsverarbeiter:innen. **Die Anforderung "Abhilfe durch Datensicherheitsmaßnahmen" ist aufgrund der umfangreichen Datensicherheitsmaßnahmen als erfüllt anzusehen.**
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:	
Stellungnahme des Datenschutzbeauftragten (Art. 35 Abs. 2 DSGVO; WP 248 Rev.01, 21 und 29)	Die Stellungnahmen der datenschutzbeauftragten Personen können eingeholt werden. **Die Anforderung "Stellungnahme des Datenschutzbeauftragten" ist aufgrund der grundsätzlichen Machbarkeit als erfüllbar anzusehen.**
Stellungnahme betroffener Personen (Art. 35 Abs. 9 DSGVO; WP 248 Rev.01, 21 und 29)	Die Stellungnahmen von betroffenen Personen oder ihren Vertretungen, wie etwa Patient:innenanwält:innen, können eingeholt werden. **Die Anforderung "Stellungnahme betroffener Personen" ist aufgrund der grundsätzlichen Machbarkeit der Einholung von Stellungnahmen als erfüllbar anzusehen.**

	Unterzeichner	Parlamentsdirektion
	Datum/Zeit-UTC	2023-11-22T16:32:22+01:00
Prüfinformation	Dieses Dokument wurde elektronisch besiegelt. Informationen zur Prüfung des elektronischen Siegels und des Ausdrucks finden Sie unter: https://www.parlament.gv.at/siegel	