Risikoanalyse und Datenschutz-Folgenabschätzung anhand des SDM Modells (Standard Datenschutzmodell) iVm Dokumentations-rastern des Bundes

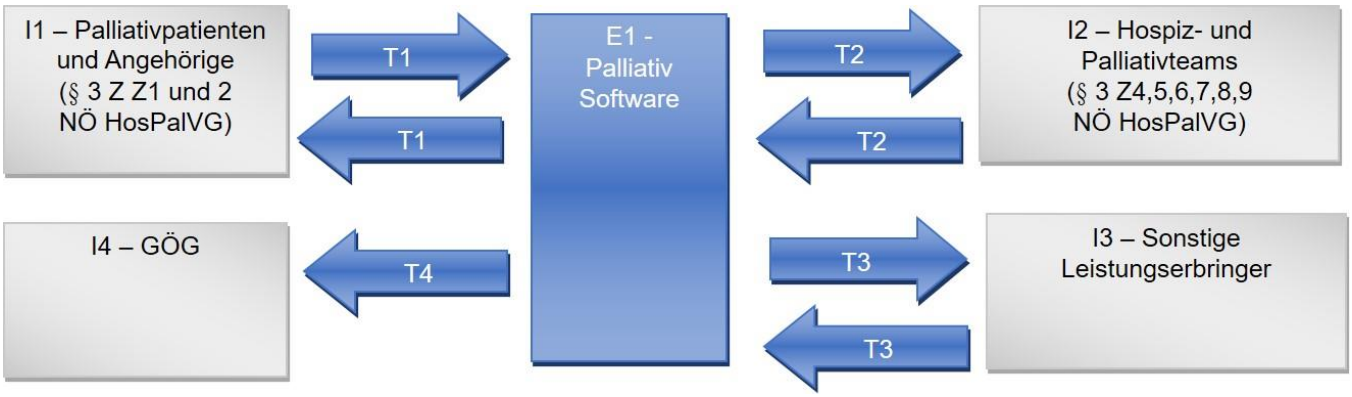
1. Kurzfassung

Anhand der Umsetzung des Gesetzes über die spezialisierte mobile Hospiz- und Palliativversorgung in Niederösterreich (NÖ HosPalVG) wird eine Risikoanalyse und von deren Ergebnis unabhängig eine Datenschutz-Folgenabschätzung für den Einsatz der für die Dokumentation empfohlenen Software durchgeführt.

2. Anwendungsbeschreibung

Um die in NÖ HosPalVG beschriebenen Ziele zu erreichen ist der Einsatz einer einheitlichen Software zur Dokumentation der Patienten und Leistungen zwingend erforderlich. Diese Software muss sowohl die jeweiligen Teamstrukturen abbilden und die Arbeit und Organisation innerhalb der Teams erfassen, als auch eine umfängliche Anamnese und Verlaufsdokumentation der behandelten Palliativpatienten und An-und Zugehörigen erlauben sowie die Dokumentation der Arbeit der Teams an den Palliativpatienten und An- und Zugehörigen abbilden.

3. Datenflussdiagramm



I3 Sonstige Leistungserbringer gemäß Art 4 Z 10 DSGVO sind andere an der Versorgung beteiligte Leistungserbringer, insbesondere Hausärzte, Apotheken, Sanitätshäuser, etc.

I4 § 10 Hospiz- und Palliativfondsgesetz (HosPalFG) idF BGBl. I Nr. 29/2022

Zusammenstellung der im Modellfall angeführten Komponenten

Subsysteme / Beteiligte	**verarbeitete Daten**	**Zweck**	**Rechts-grundlage**	**Speicher-dauer**	**Sicherheits-maßnahmen**
E1 – Pallia-tivsoftware	NÖ HosPalVG	Abwicklung des durch das Gesetz vorge-sehene Ver-fahren	NÖ HosPalVG	Speicherung von Patien-tendaten nach gesetzlichen Vorgaben	§ 9 NÖ Hos-PalVG Art. 25 und 32 DSG-VO[1]

Die Daten, die an den Schnittstellen (I1 – I3) erhoben werden sollen

Datenpaket 1	**Datenpaket 2, 3**	**Datenpaket 4**
Personenbezogene Daten Gesundheitsdaten Generalien Betreuungsdaten	Personenbezogene Da-ten Generalien Betreuungsdaten Verfahrensdaten	Gesundheitsdaten Personenbezogene Da-ten Betreuungsdaten

Die Schnittstellen der Komponenten, die darüber zugänglichen Daten und etwaige Sicherheitsei-genschaften

Schnittstellen	**Daten (1)**	**Sicherheitseigenschaften**
I1 – Palliativpatienten und An und Zugehörige § 3 Z1 und 2	NÖ HosPalVG, § 9	Art. 25 und 32 DSGVO
I2,3 – Hospiz- und Palliativ-teams, Sonstige Leistungser-bringer § 3 Z4,5,6,7,8 und 9	NÖ HosPalVG, § 9	
I4 – GÖG (2)	§ 10 Hospiz- und Palliativ-fondsgesetz (HosPalFG) idF BGBl. I Nr. 29/2022	

(1) Die Angabe der betroffenen Datenkategorien kann nur generisch erfolgen, da dies Abhän-gig von der Art des jeweiligen Hospiz- und Palliativteams und von der Art der Erkrankung und der Lebensumstände des Patienten ist.

1 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)

(2) Gemäß § 10 HosPalFG müssen Daten zur Hospiz- und Palliativversorgung an die GÖG geliefert werden.

Die Eigenschaften zwischen den Verbindungen der Komponenten

Verbindungen	**übertragene Daten (rechtliche Grundlagen: siehe Beteiligte) (1)**	**Sicherheitsmaßnahmen**
T1 – Dokumentation von Daten zu Palliativpatienten und An- und Zugehörigen durch die Leistungserbringer, Erfassung von Daten durch Patienten und An- und Zugehörige	Personenbezogene, Gesundheitsdaten; Generalien; Betreuungsdaten	Siehe E1
T2,3 – Informationen zu Palliativpatienten und deren An- und Zugehörigen, Dokumentation von Einsatz- und Leistungsdaten	Personenbezogene Daten, Generalien, Betreuungsdaten, Verfahrensdaten, Daten zur Qualifikation	
T4 – Datenlieferung laut Landesgesetz	Gesundheitsdaten, Personenbezogene Daten, Betreuungsdaten, Daten zur Qualifikation, Angaben zur Tätigkeit, Stundenausmaß, Art der Beschäftigung	Siehe E1

(1) Die Angabe der betroffenen Datenkategorien kann nur generisch erfolgen, da dies Abhängig von der Art des jeweiligen Versorgers und von der Art der Erkrankung der Lebensumstände des Patienten ist.

4. Identifikation der mit dem Verfahren befassten unmittelbaren Akteure

- Hospiz- und Palliativteams, Patienten und An- und Zugehörige (NÖ HosPalVG)
    - nicht ehrenamtliche und ehrenamtliche Mitarbeiter der Palliativ- und Hospizteams
    - betroffene Patienten und An- und Zugehörige

- Sonstige Leistungserbringer gemäß Art 4 Z10 DSGVO

- Andere an der Versorgung beteiligten Leistungserbringer insbesondere Hausärzte, Apotheken, Sanitätshäuser, etc.

- Die weiteren Beteiligten, Parteien oder Beitragenden
  - IT-Mitarbeiter der jeweiligen Institutionen
  - Support der Palliativ Software

5. Risikoanalyse und -management

5.1. Rechtsgrundlagen

Da ein Gesetzesvorhaben (Art. 6 Abs. 1 lit. c DSGVO, Art. 9 Abs. 2 lit. g und lit. j DSGVO) betrachtet wird, liegt damit auch für eine darauf basierende Datenverarbeitung eine Rechtsgrundlage vor. Aus § 1 Abs. 1 NÖ HosPalVG sowie aus den Erwägungsgründen 1, 3, 5, 10, 14, 33, 48 und 80 folgt, dass ein überwiegendes öffentliches Interesse vorliegt, sodass die angegebenen Ausnahmegründe des Art. 9 DSGVO anwendbar sind. Um die Versorgung der Patientinnen und Patienten im multiprofessionellen Team zu gewährleisten und einen Versorgungsnachweis zu erbringen ist eine strukturierte Dokumentation der Daten und Leistungsdaten der Patientinnen und Patienten sowie deren An- und Zugehörigen erforderlich.

6. Datenschutz-Folgenabschätzung

6.1. Risikoidentifikation/-bewertung

1) Leistungserbringer
   Leistungserbringer könnten erfasste vertrauenswürdige Daten einem Personenkreis zugänglich machen, der diese nicht einsehen darf **(#RN01)**.
2) Hacking
   Es könnte versucht werden, durch Eingabe von schädlichem Programmcode („CodeInjection“) Daten von Patienten zu erlangen (**#RH02**).
3) System
   Das System „E1“ könnte nicht den Art. 24, 25 und 32 DSGVO entsprechend umgesetzt worden sein, sodass Daten an Unberechtigte auch die Daten zugreifen können (**#RS01**).

6.2. Eingriffsintensität/Schutzbedarf

6.3. Bewertung des Risikos

a. Datenminimierung
   Die beschriebenen Datenpakete stellen ein Minimum zur Erreichung des Zwecks der Verarbeitung dar.

b. Verfügbarkeit

Das Risiko besteht darin, dass eine grundsätzlich zustehende Gewährung nicht ausgesprochen wird (**#RVerf01**).

c. Integrität

Hiermit ist die Richtigkeit, Aktualität und Authentizität der Daten gemeint. Diese wäre bei fehlerhaften Abfragen der Datenbank oder fehlerhaften Angaben zu den Patienten verletzt (**#RInt01**). Ein Missbrauchsrisiko der verwendeten IT Systeme besteht ebenfalls (**#RInt02**). Das Nichtvorliegen eines IT Sicherheitsmanagements wäre ebenfalls ein Risikofaktor (**#RInt03**).

d. Vertraulichkeit

Das entsprechende Risiko besteht hinsichtlich einer unbefugter Kenntnisnahme innerhalb der Institution (**#RVert01**) aufgrund falsche Rechtevergaben

e. Transparenz

Hier erscheint kein Risiko gegeben, sofern Organisationsvorschriften eine Veröffentlichung der Informationen nach Art. 13 und 14 DSGVO vorsehen.

f. Nichtverkettung

Das Verkettungsrisiko umfasst die zweckentfremdete Nutzung durch die gemeinsamen Verantwortlichen bzw. der personenbezogenen Daten aus der gemeinsamen Nutzung der Daten. Hier ist kein bzw. lediglich ein minimales Risiko gegeben, da deren unzulässige Verarbeitung mit umfassenden disziplinären oder strafrechtlichen Maßnahmen bedroht ist.

g. Intervenierbarkeit

Das Interventionsrisiko bezeichnet zwei Aspekte: Zum einen, dass ein Verfahren die Betroffenenrechte auf Berichtigung von Daten, Widerruf von Einwilligungen, Kündigung von Verträgen, Löschen von Daten und die Nachweise hierüber nicht hinreichend wirksam umsetzt (**#RIv01**). Zum anderen beschreibt es, dass eine Organisation nicht hinreichend in der Lage ist, dass Verfahren transparent, zweckgemäß und integer zu ändern, weil dies bspw. rechtlich gefordert oder technisch notwendig ist („Changemanagement“). Auf Änderungsanforderungen zu reagieren und diese intern umsetzen zu können, ist ein Aspekt, der alle beteiligten Organisationen betrifft und ein wesentlicher Prüfaspekt eines übergreifenden Datenschutzmanagements ist. (**#RIv02**).

7. Maßnahmenbestimmung

7.1. „Risikomatrix“

Hier werden die Ergebnisse des Abschnitts 6. und 7.5. zusammengefasst. Die Risikobewertung (rot, gelb, grün) kann dann zu dem genannten Ergebnis führen, wenn die angegebenen Maßnahmen gesetzt werden:

Risiko	**Schwere**	**Eintrittswahrscheinlichkeit**	**Maßnahme**
	Vernachlässigbar (V)	**Vernachlässigbar (V)**	**Akzeptanz (A)**
	Begrenzt (B)	**Begrenzt (B)**	**Reduktion (R)**
	Wesentlich (W)	**Wesentlich (W)**	**Übertragung (Ü)**
	Maximal (M)	**Maximal (M)**	**Vermeidung (V)**
#RB01	V	V	A (#MDesign01, #MZert01, #MBetr-MA01)
#RH01	B	B	R (Privacy by Design)
#RH02	B	B	R (ISO 27001)
#RH03	W	B	R (unmittelbarer Virenscan allf. Uploads)
#RInt01	V	V	A (#MDesign01, #MZert01, #MBetr-MA01)
#RInt02	W	V	A (ISO 27001)
#RInt03	V	V	A (#MDesign01, #MZert01, #MBetr-MA01)
#RIv01	V	V	A (#MDesign01, #MZert01, #MBetr-MA01)
#RIv02	V	V	A (#MDesign01, #MZert01, #MBetr-MA01)
#RN01	V	V	A (#MDesign01, #MZert01, #MBetr-

Risiko	Schwere	Eintrittswahrschein-lichkeit	Maßnahme
			MA01)
#RN02	V	V	A (#MDesign01, #MZert01, #MBetr-MA01
#RP01	V	V	A (#MDesign01, #MZert01, #MBetr-MA01)
#RS01	B	B	R (Privacy by Design)
#RTrans01	B	B	#MTrans01
#RÜm01	V	V	A (#MDesign01, #MZert01, #MBetr-MA01)
#RVerf01	V	V	A (#MDesign01, #MZert01, #MBetr-MA01)
#RVert01	B	V	A (Dienstrecht)
#RVert02	B	V	A (Dienstrecht)
#RVert03	B	V	A (Kommunikation https, verschlüsselt)
#RVert04	B	V	A (#MDesign01, #MZert01, #MBetr-MA01)
#RVert05	B	B	R (IDM Genehmi-gungsprozess)
#RVert06-#RVert12	B	B	R (#MMin01, #MVert01, #MVert02)

7.2. Dokumentation Bewertungsergebnisse

Als Ergebnis der Datenschutz-Folgenabschätzung kann festgestellt werden, dass nach Setzen der skizzierten Maßnahmen keine hohen Risiken für Rechte und Freiheiten von betroffenen Personen zu erwarten sind.

7.3. Berichterstellung

Das ULD (Datenschutzzentrum) schlägt als zusätzliche Darstellungsform folgende Tabelle vor:

Zusammenstellung von Risiken	Interne Stelle (Dritte), Externe Stelle	Hinweisgebende Person	Übermittlungsempfängerin m	Weitere Beteiligte, Parteien, Beitragende	Betroffene Person	Hacking	System
Datenminimierung							
Verfügbarkeit	#RVerf01					#RH01 #RH02	
Integrität	#RInt01 #RInt02 #RInt03	#RInt01				#RH03	
Vertraulichkeit	#RN01 #RN02 #RVert01 #RVert04 #RVert05 #RVert07 #RVert08	#RVert06 #RVert07 #RVert08 #RVert09 #RVert10 #RVert11 #RVert12	#RÜm01 #RVert02	#RP01 #RVert06 #RVert07 #RVert08 #RVert09 #RVert10 #RVert11 #RVert12	#RB01 #RVert06 #RVert07 #RVert08 #RVert09 #RVert10 #RVert11 #RVert12	#RVert03	#RS01
Transparenz		#RTrans01					
Intervenierbarkeit	#RIv01 #RIv02						
Nichtverkettung							

7.5. Bericht

BEWERTUNG DER NOTWENDIGKEIT UND VERHÄLTNISMÄSSIGKEIT

Die Bewertung hat nach EG 90 und 96, Art. 35 Abs. 7 lit. b und lit. 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"[2] des Europäischen Datenschutzausschusses (EDSA) (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: (Art. 5 Abs. 1 lit. b DSGVO)	§ 2 NÖ HosPalVG

2 https://www.dsb.gv.at/dam/jcr:ba295358-cf65-41a6-911d-a88cae94ba20/Leitlinien%20zur%20Datenschutz-Folgenabschaetzung-wp248-rev-01_de.pdf

Eindeutiger Zweck: (Art. 5 Abs. 1 lit. b DSGVO)	§ 2 NÖ HosPalVG, definiert den Zweck nicht mehrdeutig; eine unrichtige Verwendung der Daten in diesem Sinne ist ausgeschlossen.
Legitimer Zweck: (Art. 5 Abs. 1 lit. b DSGVO)	5.1. Rechtsgrundlagen
Rechtmäßigkeit der Verarbeitung: (EDSA, WP 248, 21 iVm Art. 6 DSGVO)	5.1. Rechtsgrundlagen
Angemessenheit der Verarbeitung: (EDSA, WP 248, 21 iVm Art. 5 Abs. 1 lit. c DSGVO)	§ 9 Abs. 1 NÖ HosPalVG. Der Zweck der Verarbeitung kann nicht in zumutbarer Weise durch andere Mittel erreicht werden. Ohne die Verarbeitung der in § 9 Abs. 2 NÖ HosPalVG festgelegten Daten kann ein effizienter Hinweisgeberschutz nicht erzielt werden. Art. 17 und 18 der Richtlinie (EU) 2019/1937 stellen darauf ab, dass Meldungen in der Form zu dokumentieren sind, dass eine „vollständige und genaue Niederschrift“ erfolgt. Da viele Bereiche des Unionsrechts berührt sind, hat der Gesetzesvorschlag in Bezug auf Angabe der Datenkategorien einem generischen Ansatz zu folgen.
Erheblichkeit der Verarbeitung: (EDSA, WP 248, 21 iVm Art. 5 Abs. 1 lit. c DSGVO)	§ 2 NÖ HosPalVG
Beschränktheit der Verarbeitung auf das notwendige Maß: (EDSA, WP 248, 21 iVm Art. 5 Abs. 1 lit. c DSGVO)	Die Verarbeitung ist auf das erforderliche Maß beschränkt, weil die bereitgestellten Daten von den gemeinsam Verantwortlichen gemäß Art. 4 Z 7 DSGVO und Dritten nur auf Aufforderung von Patientinnen und Patienten zur Verfügung gestellt werden.
Speicherbegrenzung: (EDSA, WP 248, 21 iVm Art. 5 Abs. 1 lit. e DSGVO)	Eine entsprechende Regelung zur Sicherstellung des datenschutzrechtlichen Grundprinzips der Speicherbegrenzung ergibt sich aus Art. 5 Abs. 1 lit. e DSGVO. Dementsprechend sind personenbezogene Daten zu löschen, sofern diese iSd Art. 17 Abs. 3 lit. e DSGVO nicht mehr erforderlich sind und für die Besorgung der Aufgaben im Sinne des NÖ HosPalVG nicht mehr benötigt werden. Da die personenbezogenen Daten (Erwägungsgrund 86) als Beweismittel herangezogen werden können, ist im Hinblick auf die mögliche Dauer derartiger (Gerichts-)verfahren nur eine „qualitative Angabe“ zur Spei-

	cherbegrenzung möglich.
Generelle Information der betroffenen Personen: (EDSA, WP 248, 21 iVm Art. 12 DSGVO)	Im Sinne der Empfehlungen des EDSA (WP 248, 21) hat eine Datenschutz-Folgenabschätzung auch die transparente Information gemäß Art. 12 DSGVO zu behandeln. Die Informationen gemäß Art. 13 und 14 DSGVO werden in den folgenden beiden Zeilen behandelt, sodass die generellen Mitteilungen gemäß Art. 15 bis 22 und 34 DSGVO verbleiben. Diese sind: – die Mitteilung gemäß Art. 15 Abs. 2 DSGVO über die geeigneten Garantien bei Übermittlung in Drittländer oder an internationale Organisationen; – gegebenenfalls die Mitteilung an die betroffene Person, dass eine Einschränkung aufgehoben wird (Art. 18 Abs. 3 DSGVO); – gegebenenfalls die Information von Empfängerinnen oder Empfängern gemäß Art. 19 DSGVO, dass eine betroffene Person die Berichtigung oder Löschung von personenbezogenen Daten oder eine Einschränkung der Verarbeitung verlangt, es sei denn, dies erweist sich als unmöglich oder ist mit einem unverhältnismäßigen Aufwand verbunden; – die Information der betroffenen Personen über die Empfängerinnen oder Empfänger ihrer personenbezogenen Daten, auf Verlangen der betroffenen Personen (Art. 19 DSGVO); – gegebenenfalls die Benachrichtigung über Verletzungen des Schutzes personenbezogener Daten gemäß Art. 34 Abs. 1 DSGVO; – Unter der Voraussetzung, dass die genannten Mitteilungen tatsächlich erfolgen, gilt die vorliegende Datenschutz-Folgenabschätzung als erfüllt im Sinne des Art. 35 Abs. 10 DSGVO.
Information der betroffenen Personen bei Erhebung: (EDSA, WP 248, 21 iVm Art. 13 DSGVO)	Die gemäß Art. 13 DSGVO erforderlichen Informationen werden wie folgt erbracht: – die Zwecke, für welche die personenbezogenen Daten verarbeitet werden sollen: durch Publikation des Gesetzesvorhabens als Landesgesetz im Landesgesetzblatt (LGBl.); – Ebenfalls durch Publikation im LGBl.: o die Rechtsgrundlage für die Verarbeitung

	○ die EmpfängerInnen bzw. Kategorien von Empfängerinnen und Empfängern ○ die Dauer, für die die personenbezogenen Daten gespeichert werden – Daher müssen diese Informationen gemäß Art. 13 Abs. 4 DSGVO nicht mehr gesondert bei Erhebung bei den betroffenen Personen zur Verfügung gestellt werden. – Mittels des Verzeichnisses von Verarbeitungstätigkeiten (www.noe.gv.at/datenschutz) wird veröffentlicht: ○ Name und Kontaktdaten der oder des Verantwortlichen, ○ die Kontaktdaten ihrer oder ihres Datenschutzbeauftragten, ○ gegebenenfalls die Absicht die personenbezogenen Daten an ein Drittland oder eine internationale Organisation zu übermitteln sowie das Vorhandensein oder das Fehlen eines Angemessenheitsbeschlusses der Kommission, ○ ein Hinweis auf das allfällige Bestehen anderer / restlicher Rechte der betroffenen Personen, ○ ein Hinweis auf das Bestehen des Rechts auf Beschwerde (Art. 77 DSGVO), ○ gegebenenfalls Informationen über das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Art. 22 Abs. 1 und 4 DSGVO sowie ○ gegebenenfalls die über eine allfällige Weiterverarbeitung erforderlichen Informationen gemäß Art. 13 Abs. 3 DSGVO – Somit gilt die vorliegende Datenschutz-Folgenabschätzung hinsichtlich der Information gemäß Art. 13 DSGVO als erfüllt im Sinne des Art. 35 Abs. 10 DSGVO.
Auskunftsrecht der betroffenen Personen: (EDSA, WP 248, 21 iVm Art. 15 DSGVO)	In den generellen Vorschriften und Erlässen sind diese Erfordernisse geregelt; nur wenn aufgrund des Gegenstands des Gesetzes Ausnahmen zulässig sind (vgl. Art. 23 DSGVO), ist dies im Gesetz auszunehmen. Da das Auskunftsrecht der betroffenen Personen gemäß Art. 15

	DSGVO wahrgenommen werden kann, sofern kein gesetzlich vorgesehener Grund dem entgegensteht, gilt die vorliegende Datenschutz-Folgenabschätzung als erfüllt im Sinne des Art. 35 Abs. 10 DSGVO.
Recht auf Datenübertragbarkeit: (Art. 20 DSGVO)	Das Recht auf Datenübertragbarkeit steht gemäß Art. 20 Abs. 1 lit. a DSGVO nicht zu, weil die Verarbeitung – weder aufgrund einer Einwilligung (Art. 6 Abs. 1 lit. a oder Art. 9 Abs. 2 lit. a DSGVO) – noch aufgrund eines Vertrags (Art. 6 Abs. 1 lit. b DSGVO) erfolgt.
Auftragsverarbeiterinnen und Auftragsverarbeiter: (Art. 28 DSGVO)	Da Art. 35 Abs. 10 DSGVO Datenschutz-Folgenabschätzungen auch im Zuge von Gesetzgebungsverfahren zulässt und die konkret zum Einsatz kommenden Auftragsverarbeiterinnen oder Auftragsverarbeiter typischerweise nicht gesetzlich geregelt sind, ist ein Verweis auf die Einhaltung der Art. 28 f DSGVO als ausreichend anzusehen.
Schutzmaßnahmen bei der Übermittlung in Drittländer: (Kapitel V DSGVO)	Dies ist bei diesem Gesetzesvorhaben nicht vorgesehen.
Vorherige Konsultation: (Art. 36 und EG 96 DSGVO)	Die Datenschutzbehörde wirkte im Rahmen des Begutachtungsverfahrens aktiv an der Gestaltung des vorliegenden Entwurfes mit.

RISIKEN Die Risiken sind nach ihrer Ursache, Art, Besonderheit, Schwere und Eintrittswahrscheinlichkeit zu bewerten (Erwägungsgründe 76, 77, 84 und 90 DSGVO, siehe auch Abschnitt III). Als Risiken werden in den Erwägungsgründen 75 und 85 DSGVO unter anderem genannt:	
Physische, materielle oder immaterielle Schäden: (EG 90 iVm 85 DSGVO) **#RVert06**	Die Wahrscheinlichkeit einer Manifestation besteht bei folgenden Risikotatbeständen: **#RN01, #RN02, #RÜm01, #RP01** § 9 Abs. 9 und 10 NÖ HosPalVG verpflichtet die Verantwortlichen zur Erfüllung der aus den datenschutzrechtlichen Regelungen erwachsenden Pflichten. Diese sind insbesondere – das Treffen von auch zum Zeitpunkt der eigentlichen Verarbeitung geeigneten technischen und organisatorischen Maßnahmen, um die Rechte der betroffenen Personen zu schützen.

	– das Anwenden von Art. 32 DSGVO, dem zu Folge müssen „der Verantwortliche und der Auftragsverarbeiter […] ein dem Risiko angemessenes Schutzniveau“ gewährleisten. – die Sanktionierung der Nichteinhaltung mit 10 Millionen Euro (Art. 83 Abs. 4 lit. a DSGVO, soweit gemäß § 30 Abs. 5 DSG anwendbar). Die Konsequenzen, die bei einem Verstoß drohen, dämmen die Risiken von physischen, materiellen oder immateriellen Schäden ebenfalls ein. Aus der Bestimmung des § 9 Abs. 10 folgt eine wesentliche Senkung des Risikos, da diese – angemessene Maßnahmen, – die Einhaltung des Datengeheimnisses (§ 6 DSG), – strenge Zweckbindung sowie – den Schutz vor Vergeltungsmaßnahmen umfasst.
Verlust der Kontrolle über personenbezogene Daten: (EG 90 iVm 85 DSGVO) **#RTrans01**	Die Wahrscheinlichkeit einer Manifestation besteht bei folgenden Risikotatbeständen: **#RH01, #RH02, #RS01, #RVerf01, #RInt01, #RInt02, #RInt03** Diesem Risiko wird durch die Einhaltung der (anwendbaren) Rechte der betroffenen Person gemäß Kapitel III der DSGVO Rechnung getragen. Das sind: – transparente Information, Kommunikation und Modalitäten für die Ausübung der Rechte der betroffenen Person (Art. 12 DSGVO), – Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person (Art. 13 DSGVO), – Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden (Art. 14 DSGVO), – Auskunftsrecht der betroffenen Person (Art. 15 DSGVO), – Recht auf Berichtigung (Art. 16 DSGVO), – Recht auf Löschung / „Recht auf Vergessenwerden“ (Art. 17 DSGVO), – Recht auf Einschränkung der Verarbeitung (Art. 18 DSGVO) sowie

	– Mitteilungspflicht im Zusammenhang mit der Berichtigung oder Löschung personenbezogener Daten oder der Einschränkung der Verarbeitung (Art. 19 DSGVO) – Außerdem sind die Datensicherheitsmaßnahmen gemäß Art. 32 DSGVO von den jeweiligen Verantwortlichen einzuhalten. Damit wird die Wahrscheinlichkeit eines Verlustes der Kontrolle über personenbezogene Daten effektiv gemindert. Eine wesentliche Senkung des Risikos erfolgt insbesondere durch Regelung – der lückenlosen Protokollierung, – des Datengeheimnisses (§ 6 DSG) sowie – der strengen Zweckbindung.
Diskriminierung: (EG 90 iVm 85 DSGVO) **#RDisk01**	Die Wahrscheinlichkeit einer Manifestation besteht bei folgenden Risikotatbeständen: **#RN01, #RN02, #Rüm01, #RP01** Eine wesentliche Senkung des Risikos erfolgt insbesondere durch – geeignete technische und organisatorische Maßnahmen gemäß Art. 25 DSGVO, – die Verpflichtung gemäß Art. 32 DSGVO, wonach Verantwortliche und Auftragsverarbeiterinnen oder Auftragsverarbeiter für ein dem Risiko angemessenes Schutzniveau sorgen müssen, – die Sanktionierung eines Verstoßes gegen Art. 32 DSGVO mit einer Geldbuße bis zu 10 Millionen Euro in Art. 83 Abs. 4 lit. a DSGVO, soweit gemäß § 30 Abs. 5 DSG anwendbar.
Identitätsdiebstahl oder -betrug: (EG 90 iVm 85 DSGVO) **#RVert07**	Die Wahrscheinlichkeit einer Manifestation besteht bei folgenden Risikotatbeständen: **#RN01, #RN02, #Rüm01, #RP01, #RH01, #RH02, #RS01, #RVerf01, #RInt01, #RInt02, #RInt03** Dieses Risiko wird insbesondere durch die unionsrechtliche Sanktionierung (siehe oben: Risiken / Physische, materielle oder immaterielle Schäden) effektiv gemindert. Eine wesentliche Senkung des Risikos erfolgt insbesondere durch Regelung – der lückenlosen Protokollierung,

	– des Datengeheimnisses (§ 6 DSG) sowie – der strengen Zweckbindung.
Finanzielle Verluste: (EG 90 iVm 85 DSGVO) **#RVert08**	Die Wahrscheinlichkeit einer Manifestation besteht bei folgenden Risikotatbeständen: **#RN01, #RN02, #RÜm01, #RP01, #RH01, #RH02, #RS01, #RVerf01, #RInt01, #RInt02, #RInt03** Dieses Risiko wird insbesondere durch die unionsrechtliche Sanktionierung (siehe oben: Risiken / Physische, materielle oder immaterielle Schäden) effektiv gemindert. Eine wesentliche Senkung des Risikos erfolgt insbesondere durch Regelung – angemessener Maßnahmen, insbesondere des Datengeheimnisses (§ 6 DSG) sowie – strenger Zweckbindung.
Unbefugte Aufhebung der Pseudonymisierung: (EG 90 iVm 85 DSGVO) **#Vert09**	Die Wahrscheinlichkeit einer Manifestation besteht bei folgenden Risikotatbeständen: **#RH01, #RH02, #RS01** Soweit im Gesetzesvorhaben eine Pseudonymisierung vorgesehen ist, erfolgt eine wesentliche Senkung des Risikos insbesondere durch – unionsrechtliche Sanktionierung (siehe oben: Risiken / Physische, materielle oder immaterielle Schäden); – Einsatz bereichsspezifischer Personenkennzeichen (§ 9 E-GovG).
Rufschädigung: (EG 90 iVm 85 DSGVO) **#RVert10**	Die Wahrscheinlichkeit einer Manifestation besteht bei folgenden Risikotatbeständen: **#RN01, #RN02, #RÜm01, #RP01, #RH01, #RH02, #RS01, #RVerf01, #RInt01, #RInt02, #RInt03** Soweit im Gesetzesvorhaben eine Pseudonymisierung vorgesehen ist, erfolgt eine wesentliche Senkung des Risikos insbesondere durch – unionsrechtliche Sanktionierung (siehe oben: Risiken / Physische, materielle oder immaterielle Schäden); – Einsatz bereichsspezifischer Personenkennzeichen (§ 9 E-GovG).

Verlust der Vertraulichkeit bei Berufsgeheimnissen: (EG 90 iVm 85 DSGVO) **#RVert11**	Vgl. **#RVert10.**
Erhebliche wirtschaftliche oder gesellschaftliche Nachteile: (EG 90 iVm 85 DSGVO) **#RVert12**	Die Wahrscheinlichkeit einer Manifestation besteht bei folgenden Risikotatbeständen: **#RN01, #RN02, #RÜm01, #RP01, #RVert01-#RVert05** Soweit im Gesetzesvorhaben eine Pseudonymisierung vorgesehen ist, erfolgt eine wesentliche Senkung des Risikos insbesondere durch – unionsrechtliche Sanktionierung (siehe oben: Risiken / Physische, materielle oder immaterielle Schäden); – Einsatz bereichsspezifischer Personenkennzeichen (§ 9 E-GovG), – sowie expliziter Regelung o des Datengeheimnisses (§ 6 DSG), o der strengen Zweckbindung, o des Schutzes vor Vergeltungsmaßnahmen.

ABHILFEMASSNAHMEN 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 DSGVO) **#MMin01**	Abschnitt 6.3.a.
Schnellstmögliche Pseudonymisierung personenbezogener Daten: (EG 28 und 78 DSGVO) **#MVert01**	Soweit im Gesetzesvorhaben eine Pseudonymisierung vorgesehen ist, kann auf die Anwendung des bereichsspezifischen Personenkennzeichens (bPK) gemäß § 9 E-GovG verwiesen werden. So dies praktikabel erscheint, kann aber eine eigene Pseudonymisierung (generischer Personenschlüssel) erfolgen.
Transparenz in Bezug auf die Funktionen und die Verarbeitung personenbezogener Daten: (EG 78 DSGVO)	Durch die Publikation des Gesetzesvorhabens im Landesgesetzblatt sowie der Materialien im Zuge des Gesetzgebungsprozesses können die Hintergründe für die zulässige Verarbeitung personenbezogener Daten im Rahmen des Gesetzesvorhabens von der Öffentlichkeit kostenlos nachvollzogen werden.

#MTrans01	
Überwachung der Verarbeitung personenbezogener Daten durch die betroffenen Personen: (EG 78 DSGVO) **#MTrans02**	Die betroffenen Personen haben durch Ausübung ihrer Rechte gemäß Kapitel III der DSGVO – das sind transparente Information, Kommunikation und Modalitäten für die Ausübung der Rechte der betroffenen Person (Art. 12 ff DSGVO) die Möglichkeit, die Verarbeitung ihrer Daten durch die Verantwortlichen zu überwachen.
Datensicherheitsmaßnahmen: (EG 78 und 83 DSGVO) **#MVert02**	Den Anforderungen des Art. 32 DSGVO entsprechende Datensicherheitsmaßnahmen sind bei Verarbeitungen im Rahmen der Umsetzung des Gesetzesvorhabens zu treffen. Da Art. 35 Abs. 10 DSGVO Datenschutz-Folgenabschätzungen auch im Zuge von Gesetzgebungsverfahren zulässt, ist ein Verweis auf die Einhaltung der Maßnahmen gemäß Art. 32 DSGVO als ausreichend anzusehen.
„Privacy by Design“ (Art. 25 DSGVO) **#MDesign01**	Das Software System ist nach den Grundsätzen der „datenschutzfreundlichen Gestaltung“ implementiert. Vgl. dazu https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf
Zertifizierung einer sicheren Datenverarbeitung **#MZert01**	Die Stelle, die für den Betrieb der Datenverarbeitung zuständig ist, stellt sicher, dass durch eine geeignete Zertifizierung (zB ISO:ITEC 27001:2013) die sichere Datenverarbeitung nachgewiesen ist. Weiters ist nachzuweisen, dass regelmäßig Rezertifizierungen durch hiezu befugte Stellen erfolgen.
Betraute MitarbeiterInnen (vgl. Art. 28 Abs. 3 lit. b DSGVO) **#MBetrMA01**	Zur Verarbeitung der personenbezogenen Daten betraute Mitarbeiterinnen oder Mitarbeiter (bei der oder dem Verantwortlichen selbst bzw. einer Auftragsverarbeiterin oder einem Auftragsverarbeiter) sind zur Vertraulichkeit in der Form verpflichtet, dass ein Zuwiderhandeln wirksame (dienst)rechtliche Maßnahmen zur Folge hat. Wesentlicher Bestandteil dieser Betrauung sind geeignete Schulungsmaßnahmen, die zur Einhaltung der datenschutzrechtlichen Vorgaben beitragen und eine entsprechende Sensibilisierung zur Folge haben.

BERÜCKSICHTIGUNG VON DATENSCHUTZINTERESSEN

Gemäß Art. 35 Abs. 2 und 9 sowie Art. 36 Abs. 4 DSGVO ist – wenn möglich – der Rat der oder des Datenschutzbeauftragten einzuholen und sind die betroffenen Personen anzuhören:	
Stellungnahme der Daten-schutzbehörde: (Art. 36 Abs. 4 DSGVO)	
Stellungnahme der oder des Datenschutzbeauftragten der erlassenden Stelle (Art. 35 Abs. 2 DSGVO)	
Stellungnahme betroffener Personen: (Art. 35 Abs. 9 DSGVO)	

8. Fazit

Nach Art. 36 Abs. 1 DSGVO ist vor der Verarbeitung die Aufsichtsbehörde zu konsultieren, wenn die Verarbeitung ein hohes Risiko zur Folge hat und die oder der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft.

Da die Risikobewertung unter Berücksichtigung der gesetzten Maßnahmen ergeben hat, dass insgesamt für die Rechte und Freiheiten der oder des Betroffenen überschaubare Risiken bestehen, ist dieser Schritt nicht erforderlich.