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

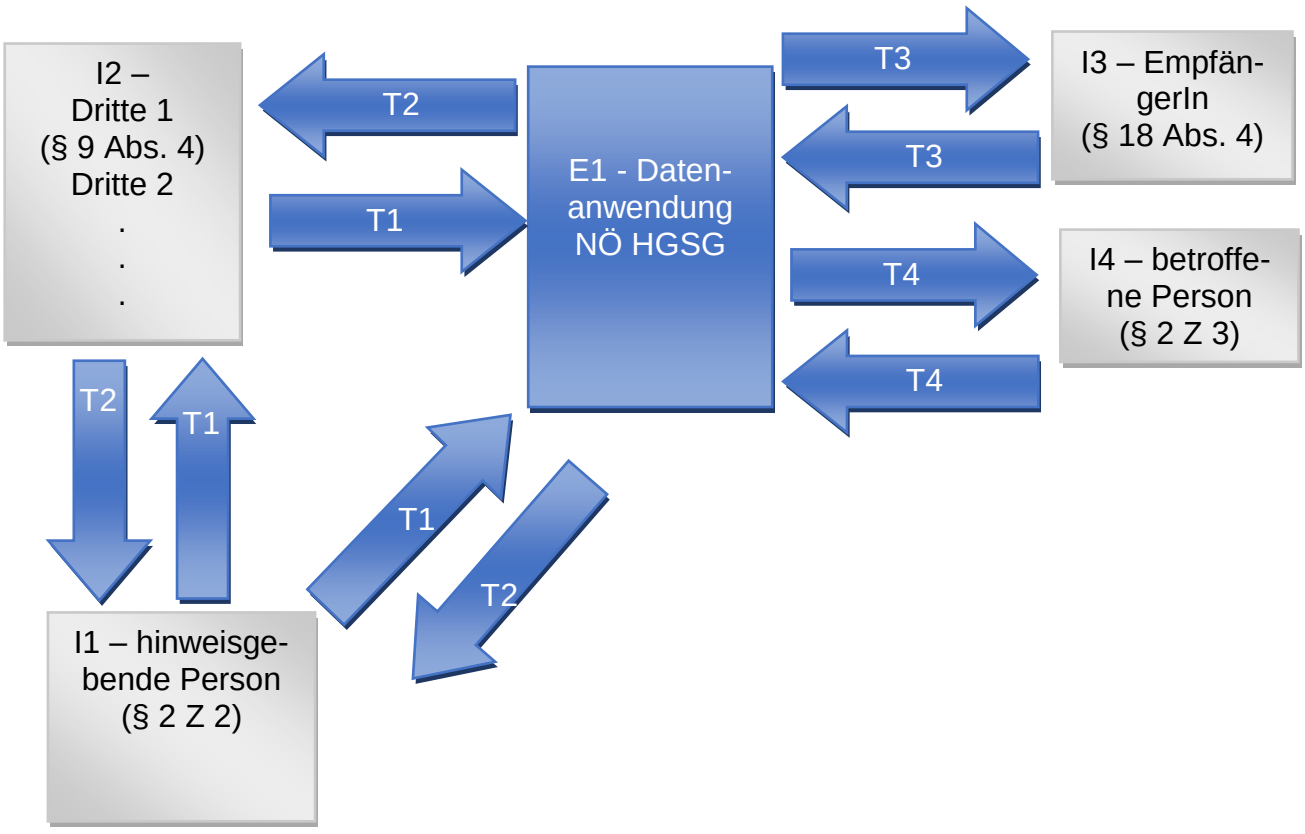
1. Kurzfassung

Anhand der Umsetzung des NÖ Hinweisgeberschutzgesetzes (NÖ HGSG) wird eine Risikoanalyse und von deren Ergebnis unabhängig eine Datenschutz-Folgenabschätzung durchgeführt.

2. Anwendungsbeschreibung

Unter bestimmten, im NÖ HGSG genannten Voraussetzungen sind interne und externe Hinweisgebersysteme einzurichten, sodass eine Person, die im Zusammenhang mit ihrer beruflichen Tätigkeit Informationen über Verstöße gegen Unionsrecht erlangt, diese melden oder offenlegen kann. Der Zweck der analysierten Datenverarbeitung ist die Erfassung der Daten der hinweisgebenden Person sowie die von der Meldung betroffenen Person zur Bearbeitung der einlangenden Meldungen über Verstöße nach den Bestimmungen des NÖ HGSG.

3. Datenflussdiagramm



Zusammenstellung der im Modellfall angeführten Komponenten

Subsysteme / Beteiligte	verarbeitete Daten	Zweck	Rechts-grundlage	Speicher-dauer	Sicherheits-maßnahmen

E1 – Daten-anwendung	NÖ HGSG, insb. § 18	Abwicklung des durch das Gesetz vorge-sehene Ver-fahren	NÖ HGSG	NÖ HGSG, insb. § 18 Abs. 5	§ 18 NÖ HGSG iVm Art. 25 und 32 DSGVO[1]

Die Daten, die an den Schnittstellen (I1 – I4) erhoben werden sollen

Datenpaket 1	**Datenpaket 2**	**Datenpaket 3**	**Datenpaket 4**
Personenbezogene Daten Sensible Daten Generalien Verfahrensdaten	Folgemaßnahmen Verfahrensdaten Entscheidungsdaten (Rückmeldung)	Übermittlungsdaten Verfahrensdaten	Innerorganisatorische Daten Verfahrensdaten

Die Schnittstellen der Komponenten, die darüber zugänglichen Daten und etwaige Sicherheitseigenschaften

Schnittstellen	**Daten (1)**	**Sicherheitseigenschaften**
I1 – hinweisgebende Person § 2 Z 2	NÖ HGSG, insb. § 18	§§ 7 Abs. 5 erster Satz, 9 Abs. 5 und 13 Abs. 6 NÖ HGSG iVm Art. 25 und 32 DSGVO
I2 – Dritte 1, 2,… (2)	NÖ HGSG, insb. § 18 iVm § 9 Abs. 5	
I3 – EmpfängerIn (3)	NÖ HGSG, insb. § 18 Abs. 4	
I4 – betroffene Person, sonstige Beteiligte (natürliche oder juristische Personen)	NÖ HGSG, insb. § 18	

(1) Die Angabe der betroffenen Datenkategorien kann nur generisch erfolgen, da dies vom unterschiedlichen Charakter der Hinweismeldung abhängt.

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) Je nach Ausgestaltung der Aufgaben des Dritten gemäß § 9 Abs. 4 handelt es sich um eine eigenständige Verantwortliche oder einen eigenständigen Verantwortlichen bzw. eine Auftragsverarbeiterin oder einen Auftragsverarbeiter. Im ersten Fall ist gegebenenfalls eine Zweckbindung und Vertraulichkeit zu den dabei berührten personenbezogenen Daten festzulegen; im zweiten ist der Abschluss einer Auftragsverarbeitervereinbarung gemäß Art. 28 Abs. 3 DSGVO erforderlich.
(3) Sofern die Bearbeitung des Hinweises ergeben hat, dass diesbezügliche Meldepflichten vorliegen (Dienstbehörden, Strafverfolgungsbehörden), ist diesen nachzukommen. Diese Stellen und Behörden agieren als Übermittlungsempfängerinnen oder Übermittlungsempfänger im datenschutzrechtlichen Sinne eigenständig verantwortlich und verarbeiten die Daten dann im Rahmen ihres gesetzlichen Auftrags.

Die Eigenschaften zwischen den Verbindungen der Komponenten

Verbindungen	**übertragene Daten (rechtliche Grundlagen: siehe Beteiligte) (1)**	**Sicherheitsmaßnahmen**
T1 – Meldung	Personenbezogene, sensible Daten; Generalien; Verfahrensdaten	Siehe E1
T2 – Rückmeldung	Folgemaßnahmen Verfahrensdaten Entscheidungsdaten (Rückmeldung) s. auch T1	
T3 – EmpfängerIn	Übermittlungsdaten Verfahrensdaten s. auch T1 und T2	
T4 – betroffene Person	Innerorganisatorische Daten Verfahrensdaten s. auch T1 und T2	

(1) Die Angabe der betroffenen Datenkategorien kann nur generisch erfolgen, da dies vom unterschiedlichen Charakter der Hinweismeldung abhängt.

4. Identifikation der mit dem Verfahren befassten unmittelbaren Akteure

- Die interne Stelle iSd §§ 9 ff NÖ HGSG, die externe Stelle iSd §§ 12 ff NÖ HGSG und ggf. Dritte iSd § 9 Abs. 4 NÖ HGSG als BetreiberInnen der Verfahren
    - MitarbeiterInnen der LAD1-IT
    - MitarbeiterInnen der Fachabteilung
    - MitarbeiterInnen der Verantwortlichen
- ÜbermittlungsempfängerInnen *m*
    - MitarbeiterIn verantwortliche EmpfängerIn *m*
    - AuftragsverarbeiterIn EmpfängerIn *m*; in Abhängigkeit von der gewählten Auftragsverarbeiterin oder dem gewählten Auftragsverarbeiter sind bei Vorliegen einer Drittlandübermittlung die neuen Standardvertragsklauseln in den Vertrag einzubeziehen [https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX:32021D0914&locale=de]*)*
- Die weiteren Beteiligten, Parteien oder Beitragenden
    - MitarbeiterInnen, organwaltende Personen, Beteiligte, Parteien, Zeugen, hinweisgebende Personen, betroffene Personen (natürliche oder juristische Personen)

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 HGSG 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. Sofern ein der Strafverfolgung zuzuführendes Tatbild verwirklicht wurde, werden im Rahmen der „Folgemaßnahmen“ gemäß § 2 Z 9 NÖ HGSG durch die zuständige Stelle geeignete Anzeigen bei der zuständigen Strafbehörde eingeleitet. Strafdaten iSd Art. 10 DSGVO werden daher nicht durch die externe, interne oder zuständige Stelle verarbeitet, sondern als „Verdachtsdaten“ in Form einer Anzeige übermittelt.

6. Datenschutz-Folgenabschätzung

6.1. Risikoidentifikation/-bewertung

1) Die interne Stelle iSd §§ 9 ff NÖ HGSG, die externe Stelle iSd §§ 12 ff NÖ HGSG und ggf. Dritte iSd § 9 Abs. 4 NÖ HGSG als BetreiberInnen der Verfahren

   Es sind Konstellationen denkbar, dass Mitarbeiterinnen oder Mitarbeiter Daten verändern, so-

dass Vorteile oder Nachteile betroffener Personen entstehen **(#RN01**) oder Daten an Nichtberechtigte übermittelt werden (**#RN02**).

a) MitarbeiterInnen LAD1-IT
b) MitarbeiterInnen Fachabteilung
c) MitarbeiterInnen der Verantwortlichen

2) ÜbermittlungsempfängerInnen *m*

Es könnten die übermittelten Daten an Nichtberechtigte weitergegeben werden (**#RÜm01**).

a) MitarbeiterIn verantwortlicher EmpfängerIn *m*
b) AuftragsverarbeiterIn EmpfängerIn *m*

3) Die weiteren Beteiligten, Parteien oder Beitragenden

Durch Falschangaben könnte eine „unbescholtene Person“ Folgemaßnahmen zugeführt werden (**#RP01**).

a) MitarbeiterInnen, organwaltende Personen, Beteiligte, Parteien, Zeugen, hinweisgebende Personen, betroffene Personen (natürliche oder juristische Personen)

4) Die betroffene Person

Durch Falschangaben könnten zur „Verteidigung“ unbeteiligte Dritte belastet werden (**#RB01**).

5) Hacking

Es könnte versucht werden, durch Eingabe von schädlichem Programmcode („CodeInjection“) weitere Daten von betroffenen Personen zu beschädigen (**#RH01**). Es könnten ungesicherte Mails gelesen werden (**#RH02**). Es könnten mit Viren infizierte Dateien hochgeladen werden (**#RH03**).

6) System

Das System „E1“ könnte nicht den Art. 24, 25 und 32 DSGVO entsprechend umgesetzt worden sein, sodass Daten an Nichtberechtigte übermittelt werden (**#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 der hinweisgebenden

Person 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 verarbeitenden Behörde (**#RVert01**), der Übermittlungsempfängerin oder des Übermittlungsempfängers *m* (**#RVert02**), aufgrund „abgehörter" Übermittlungen an die Übermittlungsempfängerin oder den Übermittlungsempfänger *m* (**#RVert03**) sowie „abgehörter" Datenverkehr zu oder von der Datenbank (**#RVert04**). Bezüglich des Zugriffs über PVP oder Identitätsmanagementsysteme (IDM) könnten unzulässige Berechtigungen vergeben werden (**#RVert05**).

e. Transparenz

Hier erscheint kein Risiko gegeben, sofern Organisationsvorschriften eine Veröffentlichung der Informationen nach Art. 13 und 14 DSGVO vorsehen und sofern es § 18 Abs. 7 NÖ HGSG vorsieht.

f. Nichtverkettung

Das Verkettungsrisiko umfasst die zweckentfremdete Nutzung des Verfahrens bzw. der personenbezogenen Daten des Verfahrens. 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, das 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	Eintrittswahrschein-lichkeit	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 Vi-renscan 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-MA01)
#RN02	V	V	A (#MDesign01, #MZert01, #MBetr-MA01
#RP01	V	V	A (#MDesign01, #MZert01, #MBetr-MA01)

Risiko	Schwere	Eintrittswahrschein-lichkeit	Maßnahme
#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:

Zusam-menstel-lung von Risiken	Interne Stelle (Dritte), Externe Stelle	Hinweis-gebende Person	Übermitt-lungs-empfän-gerIn m	Weitere Beteilig-te, Par-teien, Beitra-gende	Betroffe-ne Per-son	Hacking	System
Datenmi-nimie-rung							

Zusammenstellung von Risiken	Interne Stelle (Dritte), Externe Stelle	Hinweisgebende Person	Übermittlungsempfängerin m	Weitere Beteiligte, Parteien, Beitragende	Betroffene Person	Hacking	System
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)	§ 1 Abs. 1 NÖ HGSG
Eindeutiger Zweck: (Art. 5 Abs. 1 lit. b DSGVO)	§ 1 Abs. 2 NÖ HGSG, definiert den Zweck nicht mehrdeutig; eine unrichtige Verwendung der Daten in diesem Sinne ist ausgeschlossen.
Legitimer Zweck:	5.1. Rechtsgrundlagen, Umsetzungshinweis § 21 NÖ HGSG

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

(Art. 5 Abs. 1 lit. b DSGVO)	
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)	§ 18 Abs. 1 NÖ HGSG. Der Zweck der Verarbeitung kann nicht in zumutbarer Weise durch andere Mittel erreicht werden. Ohne die Verarbeitung der in § 18 Abs. 3 NÖ HGSG 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. Eine allgemeine Regel als Ausfluss der Umsetzung des Art. 17 letzter Satz der Richtlinie (EU) 2019/1937 ist durch § 18 Abs. 5 NÖ HGSG gegeben.
Erheblichkeit der Verarbeitung: (EDSA, WP 248, 21 iVm Art. 5 Abs. 1 lit. c DSGVO)	§ 1 NÖ HGSG; Umsetzungspflicht, auf die Richtlinie (EU) 2019/1937 gegründet. Wie oben ausgeführt ist eine Zweckerreichung ohne die in § 18 Abs. 3 NÖ HGSG angeführten Daten nicht möglich. Weiters ist zu betonen, dass die „genaue Dokumentationspflicht“ nach Art. 18 bzw. Erwägungsgrund 86 der Richtlinie (EU) 2019/1937 es erforderlich machen, den Begriff der Erheblichkeit flexibel und womöglich auf den Einzelfall abgestellt zu sehen. Da insbesondere Erwägungsgrund 86 auf „Abrufbarkeit“ und „Geeignetheit als Beweismittel“ abstellt, wird auch aus diesem Gesichtspunkt heraus auf eine gewisse Dynamik des Erheblichkeitsbegriffs abzustellen sein; die im Gesetzesvorschlag angeführten Datenkategorien entsprechen einem als erheblich zu sehenden „Minimalset“ generischer Kategorisierungen.
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, Dritten (Art. 4 Z 10 DSGVO) nur unter den Auflagen des § 18 Abs. 4 NÖ HGSG zur Kenntnis gebracht werden dürfen.
Speicherbegrenzung:	Eine entsprechende Regelung zur Sicherstellung des datenschutz-

(EDSA, WP 248, 21 iVm Art. 5 Abs. 1 lit. e DSGVO)	rechtlichen Grundprinzips der Speicherbegrenzung (Art. 5 Abs. 1 lit. e DSGVO) ergibt sich aus § 18 Abs. 5 NÖ HGSG. 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 HGSG 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 Speicherbegrenzung 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); – der Hinweis, dass Betroffenenrechte gemäß Art. 23 DSGVO ausgeschlossen sind; dies ist gemäß § 18 Abs. 8 NÖ HGSG, im Wesentlichen bis zum Abschluss der Bearbeitung des Hinweises vorgesehen. Diese Information wird auf der Homepage des Landes bekannt gemacht; – gegebenenfalls die Benachrichtigung über Verletzungen des

	Schutzes personenbezogener Daten gemäß Art. 34 Abs. 1 DSGVO; – Das Gesetz sieht in den §§ 11 und 14 NÖ HGSG Informationspflichten vor; – 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 o die EmpfängerInnen bzw. Kategorien von EmpfängerInnen o 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: o Name und Kontaktdaten der oder des Verantwortlichen, o die Kontaktdaten ihrer oder ihres Datenschutzbeauftragten, o 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, o ein Hinweis auf das allfällige Bestehen anderer / restlicher Rechte der betroffenen Personen, o ein Hinweis auf das Bestehen des Rechts auf Be-

	schwerde (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.
Information der betroffenen Personen, wenn die Daten nicht bei ihnen erhoben werden: (EDSA, WP 248, 21 iVm Art. 14 DSGVO)	Siehe oben: Bewertung / Generelle Informationen der betroffenen Personen. Gemäß den Bestimmungen des § 18 Abs. 8 Z 1 NÖ HGSG findet die Informationsobliegenheit gemäß Art. 14 DSGVO keine Anwendung, solange dies zum Schutz einer hinweisgebenden Person bzw. zur Erreichung des in § 18 Abs. 3 NÖ HGSG genannten Zwecks erforderlich ist. Art. 23 DSGVO räumt dem Gesetzgeber ein, die Anwendbarkeit von Rechten betroffener Personen nach den Bestimmungen der DSGVO einzuschränken. Art. 2 der umzusetzenden Richtlinie definiert den sachlichen Anwendungsbereich in Verstöße, die in den Anwendungsbereich der im Anhang angeführten Rechtsakte der Union fallen (a), finanziellen Interessen der Union im Sinne von Artikel 325 AEUV (b) und Verstöße gegen die Binnenmarktvorschriften im Sinne von Artikel 26 Absatz 2 AEUV (c). Begründend ist daher der Schutz sonstiger wichtiger Ziele des allgemeinen öffentlichen Interesses der Union oder eines Mitgliedstaats (Vermeidung von Verstößen gegen das Unionsrecht bzw. das Ziel der Förderung der Rechtmäßigkeit der Verwaltung) und der Schutz der Rechte und Freiheiten anderer Personen (v.a. der Schutz der hinweisgebenden Person) zu nennen (siehe Art. 23 Abs. 1 lit. e und i der 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 (siehe oben).

	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: (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** § 18 Abs. 1 und Abs. 2 NÖ HGSG verpflichten 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 schüt-

	zen. – 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 § 18 Abs. 2 NÖ HGSG folgt eine wesentliche Senkung des Risikos, da diese – angemessene Maßnahmen, – die Einhaltung des Datengeheimnisses, – strenge Zweckbindung sowie – den Schutz vor Vergeltungsmaßnahmen (§ 15) 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 (soweit nicht gemäß § 18 Abs. 8 NÖ HGSG ausgeschlossen): – die Informationspflichten gemäß §§ 11 und 14 NÖ HGSG, – 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 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, – eine explizite Regelung im Gesetzesvorhaben o insbesondere des Datengeheimnisses, o strenger Zweckbindung sowie o des Schutzes vor Vergeltungsmaßnahmen (§ 15 NÖ HGSG)
Identitätsdiebstahl oder -betrug:	Die Wahrscheinlichkeit einer Manifestation besteht bei folgenden Risikotatbeständen:

(EG 90 iVm 85 DSGVO) **#RVert07**	**#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 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, – strenger Zweckbindung sowie – des Schutzes vor Vergeltungsmaßnahmen (§ 15 NÖ HGSG).
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)	Die Wahrscheinlichkeit einer Manifestation besteht bei folgenden Risikotatbeständen:

#RVert10	**#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, o der strengen Zweckbindung, o des Schutzes vor Vergeltungsmaßnahmen (§ 15).

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 Pseudo-	Soweit im Gesetzesvorhaben eine Pseudonymisierung vorgese-

nymisierung personenbezogener Daten: (EG 28 und 78 DSGVO) **#MVert01**	hen 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) **#MTrans01**	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.
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), soweit diese nicht gemäß § 18 Abs. 8 NÖ HGSG ausgeschlossen sind – 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	Zur Verarbeitung der personenbezogenen Daten betraute Mitarbeiterinnen oder Mitarbeiter (bei der oder dem Verantwortlichen

DSGVO) **#MBetrMA01**	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 Datenschutzbehörde: (Art. 36 Abs. 4 DSGVO)	Eine Stellungnahme der Datenschutzbehörde wurde berücksichtigt.
Stellungnahme der oder des Datenschutzbeauftragten der erlassenden Stelle (Art. 35 Abs. 2 DSGVO)	Eine Stellungnahme der oder des Datenschutzbeauftragten wurde berücksichtigt.
Stellungnahme betroffener Personen: (Art. 35 Abs. 9 DSGVO)	Allfällige Stellungnahmen wurden berücksichtigt.

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.