

Anhang zur Wirkungsorientierten Folgenabschätzung:**Datenschutz-Folgenabschätzung zum Bundesgesetz über das Verfahren und den Schutz bei Hinweisen auf Rechtsverletzungen in bestimmten Rechtsbereichen (Hinweisgeberschutzgesetz – HSchG)**

Nach Erwägungsgrund 92 und Art. 35 Abs. 10 DSGVO dürfen Datenschutz-Folgenabschätzungen auch auf abstrakter Ebene durchgeführt werden. Die folgende Datenschutz-Folgenabschätzung betrifft die Verarbeitung personenbezogener Daten der Hinweisgeberinnen und Hinweisgeber, der von der Hinweisgebung betroffenen Personen sowie der von Folgemaßnahmen betroffenen oder in Folgemaßnahmen involvierten Personen. Eine Datenschutz-Folgenabschätzung ist gemäß Art. 35 Abs. 3 Buchstabe b DSGVO erforderlich, weil es potentiell auch zu einer (geographisch) umfangreichen Verarbeitung von personenbezogenen Daten kommen kann und diese auch die genannten Personen betreffen können, die besonders schutzwürdig sind.

SYSTEMATISCHE BESCHREIBUNG der geplanten Verarbeitungsvorgänge, Zwecke sowie berechtigten Interessen <i>Die Beschreibung hat nach EG 90 sowie Art. 35 Abs. 7 Buchstabe a und Abs. 8 DSGVO sowie den Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679 der Artikel-29-Datenschutzgruppe (WP 248) zu enthalten:</i>	
Art der Verarbeitung: (EG 90 DSGVO)	<p>Nach § 8 Abs. 2 HSchG sind Hinweisgeberinnen und Hinweisgeber, interne und externe Stellen, die Leitung eines Unternehmens in den Fällen des § 13 Abs. 2 HSchG sowie um Austausch oder Übermittlung personenbezogener Daten ersuchte Behörden ermächtigt, personenbezogene Daten für Zwecke des HSchG (§ 1 und Abs. 2 Z 1 HSchG) und der aufgrund des HSchG erlassenen Verordnungen zu verarbeiten.</p> <p>Die Verarbeitung darf sowohl in Papierform als auch in automationsunterstützter Form erfolgen. Besondere Formen, die aufgrund ihres Spannungsverhältnisses zu Bestimmungen der DSGVO, wie insbesondere Art. 5 DSGVO, einer gesetzlichen Regelung bedürften, wie etwa Big Data, sind nicht vorgesehen und damit nicht zulässig.</p>
Umfang der Verarbeitung: (EG 90 DSGVO)	<p>Die Verarbeitung von Daten nach § 8 Abs. 2 HSchG umfasst Daten in Zusammenhang mit Hinweisen auf Rechtsverletzungen; das sind Daten zur Person der Hinweisgeberin oder des Hinweisgebers sowie zur Person, die von der Hinweisgebung betroffen ist. Die Daten müssen der Bearbeitung einlangender Hinweise und der Beurteilung ihrer Stichhaltigkeit dienen und im öffentlichen Interesse liegen, Rechtsverletzungen zu verhindern oder zu ahnden. Nur Daten, die zur Feststellung und Ahndung einer Rechtsverletzung benötigt werden, dürfen verarbeitet werden.</p> <p>Von der Verarbeitung nach § 8 Abs. 2 HSchG umfasst sind auch Daten über gerichtlich oder verwaltungsbehördlich strafbare Handlungen oder Unterlassungen, insbesondere auch über den Verdacht der Begehung von Straftaten, sowie über strafrechtliche Verurteilungen oder vorbeugende Maßnahmen gemäß Art. 10 DSGVO.</p> <p>§ 8 Abs. 3 HSchG ermächtigt zur Verarbeitung besonderer Kategorien personenbezogener Daten nach Art. 9 Abs. 1 DSGVO unter der Voraussetzung, dass die Verarbeitung zur Erreichung der Zwecke des HSchG (§ 1 und Abs. 2 Z 1 HSchG) unbedingt erforderlich und das öffentliche Interesse an der Verarbeitung zur Erreichung dieser Zwecke erheblich</p>

	ist.
Kontext der Verarbeitung: (Art-29-Datenschutzgruppe, WP 248, 21)	Die Verarbeitung der Daten erfolgt im Kontext der Zwecke der Art. 6 Abs. 1 lit e und Art. 9 Abs. 2 lit f und g DSGVO. Mit dem HSchG, das Unionsrecht zur Grundlage hat (Richtlinie 2019/1937/EU zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden), sollen im öffentlichen Interesse der Schutz und das Verfahren bei Hinweisen auf Rechtsverletzungen gestärkt werden. Dadurch entstehen zusätzliche Anreize und Möglichkeiten, Rechtsverletzungen zu verhindern bzw. zu ahnden.
Zweck der Verarbeitung: (Art. 35 Abs. 7 Buchstabe a DSGVO)	Die Verarbeitung der Daten erfolgt im öffentlichen Interesse der Herstellung rechtmäßiger Situationen in gesellschaftlich wichtigen Bereichen (§1 HSchG). Gutgläubige Hinweise befördern diese Situationen. Die in ihnen enthaltenen Daten werden zur Ermittlung und weiteren Verfolgung der in einem Hinweis vorgeworfenen Rechtsverletzung benötigt.
Empfängerinnen und Empfänger: (Art-29-Datenschutzgruppe, WP 248, 21)	Als Empfängerinnen und Empfänger von in Hinweisen enthaltenen Daten kommen nach dem HSchG in Frage: <ul style="list-style-type: none"> – nach § 11 HSchG interne Stellen in juristischen Personen des öffentlichen und des privaten Rechts im Sinne des § 5 Z. 6 und 6 HSchG, – die Leitung eines Unternehmens in den Fällen des § 13 Abs. 2 HSchG, – externe Stellen zur Entgegennahme und Behandlung von Hinweisen gem. § 15 HSchG und – Behörden, die zur Weiterverfolgung eines Hinweises in Hinweisen enthaltenen Daten übermittelt bekommen.
Speicherdauer: (Art-29-Datenschutzgruppe, WP 248, 21)	Personenbezogene Daten sind ab ihrer letztmaligen Verarbeitung oder Übermittlung jedenfalls dreißig Jahre aufzubewahren (§ 8 Abs. 9 HSchG). Diese Frist orientiert sich an der längsten, für Verfahren der Rechtsdurchsetzung relevanten Verjährungsfrist. Falls ein Verfahren der Rechtsdurchsetzung innerhalb der dreißig Jahre begonnen hat und über diesen Zeitraum hinaus andauert, dauert die Speicherfrist bis zum Abschluss des verwaltungsbehördlichen oder gerichtlichen Verfahrens. Nach Entfall der Aufbewahrungspflicht sind personenbezogene Daten zu löschen. Protokolldaten sind ab ihrer letztmaligen Verarbeitung oder Übermittlung bis drei Jahre nach Entfall der Pflicht zur Aufbewahrung personenbezogener Daten aufzubewahren.
Funktionelle Beschreibung der Verarbeitung: (Art. 35 Abs. 7 Buchstabe a DSGVO)	Das HSchG schreibt grundsätzlich keine spezifische Form der Datenverarbeitung vor. Die Systeme der internen Hinweisgebung (§ 12 Abs. 1) wie die der bereits bestehenden externen Stellen (§ 4 Abs. 3, § 15 Abs. 1, § 17 Abs. 1 HSchG) müssen jedoch ihrer Art nach bei der Datenverarbeitung die Vertraulichkeit der Daten gewährleisten können. Die neu einzurichtenden externen Stellen müssen standardisierte, dem Stand der Technik entsprechende Whistleblower- Soft- und Hardware verwenden (§ 16 Abs. 3 HSchG). Alle externen Stellen müssen zur Einhaltung der Standards zum Schutz qualifizierter Informationen in der Lage sein (§ 17 Abs. 1 HSchG).
Beschreibung der Anlagen	Da Art. 35 Abs. 10 DSGVO

<p>(Hard- und Software bzw. sonstige Infrastruktur): (Art-29-Datenschutzgruppe, WP 248, 21)</p>	<p>Datenschutzfolgenabschätzungen auch im Zuge von Gesetzgebungsverfahren zulässt und die konkret zum Einsatz kommende Infrastruktur typischerweise nicht gesetzlich geregelt ist, ist insgesamt an dieser Stelle ein Verweis auf die Einhaltung der Maßnahmen gemäß Art. 25 und 32 DSGVO als ausreichend anzusehen.</p> <p>Die gemäß § 15 Abs. 2 und 3 HSchG neu einzurichtenden externen Stellen müssen standardisierte, dem Stand der Technik entsprechende Whistleblower- Soft- und Hardware verwenden (§ 16 Abs. 3 HSchG).</p>
<p>Eingehaltene, gemäß Art. 40 DSGVO genehmigte Verhaltensregeln: (Art-29-Datenschutzgruppe, WP 248, 21)</p>	<p>Informationen und Anleitungen auch zum Datenschutz sind gem. § 10 HSchG von juristischen Personen des öffentlichen und des privaten Rechts sowie von externen Stellen zur Verfügung zu stellen. Ein Einvernehmen mit der Datenschutzbehörde wird herzustellen sein.</p>
<p>BEWERTUNG der Notwendigkeit und Verhältnismäßigkeit <i>Die Bewertung hat nach EGen 90 und 96, Art. 35 Abs. 7 Buchstaben b und d DSGVO sowie den Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679 der Artikel-29-Datenschutzgruppe (WP 248) auf Maßnahmen</i></p> <ul style="list-style-type: none"> – <i>betreffend Notwendigkeit und Verhältnismäßigkeit (Art. 5 und 6 DSGVO) sowie</i> – <i>zur Stärkung der Rechte der betroffenen Personen (Art. 12 bis 21, 28, 36 und Kapitel V DSGVO) abzustellen.</i> 	
<p>Festgelegter Zweck: (Art. 5 Abs. 1 Buchstabe b DSGVO)</p>	<p>Die Zwecke der Datenerhebung und -übermittlung sind in den §§ 1 sowie 8 Abs. 2 und 3 HSchG festgelegt.</p>
<p>Eindeutiger Zweck: (Art. 5 Abs. 1 Buchstabe b DSGVO)</p>	<p>Der Zweck ist durch seine Definition in § 1 HSchG, durch die Festlegung des persönlichen und sachlichen Geltungsbereichs und durch die datenschutzrechtlichen Bestimmungen des § 8 HSchG über die Voraussetzungen der Zulässigkeit der Datenverarbeitung eindeutig.</p>
<p>Legitimer Zweck: (Art. 5 Abs. 1 Buchstabe b DSGVO)</p>	<p>Der Zweck ist auch im Hinblick auf die Zulässigkeit der Verarbeitung besonderer Kategorien personenbezogener Daten legitim. Die Datenverarbeitung liegt im wichtigen öffentlichen Interesse, durch Hinweisgebung strafbare Handlungen zu verhindern und aufzudecken und durch das Bestehen von Hinweisgebersystemen von der Begehung strafbarer Handlungen abzuhalten. Den Anwendungen der Datenverarbeitung nach dem HSchG liegt zudem der Zweck zugrunde, die nach den bisherigen Erfahrungen mit Whistleblowing häufigen Akte der Einschüchterung und Vergeltung zu verhindern und zu ahnden.</p> <p>Die Zwecke der Datenverarbeitung nach dem HSchG unterstützen die Einhaltung von Rechtsvorschriften und damit das Funktionieren der rechtsstaatlichen Ordnung überhaupt.</p>
<p>Rechtmäßigkeit der Verarbeitung: (Art-29-Datenschutzgruppe, WP 248, 21 iVm Art. 6 DSGVO)</p>	<p>Die Rechtmäßigkeit der Verarbeitung entsprechend Art. 6 Abs. 1 Buchstabe e DSGVO ergibt sich daraus, dass das HSchG eine Datenverarbeitung zur Wahrnehmung einer Aufgabe im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt vorsieht. Hinsichtlich des wichtigen öffentlichen Interesses des Hinwirkens auf die Einhaltung von Rechtsvorschriften wird auf die Ausführungen zu Bewertung/Legitimer Zweck verwiesen.</p>
<p>Angemessenheit der Verarbeitung: (Art-29-Datenschutzgruppe, WP 248, 21 iVm Art. 5 Abs. 1 Buchstabe c DSGVO)</p>	<p>Die Art der verarbeitbaren Daten ist nicht eingeschränkt, die Speicherdauer wie in Systematische</p>

	Beschreibung/Speicherdauer ausgeführt begrenzt. Die Verarbeitung ist im Hinblick auf den Zweck des HSchG, im Rahmen des persönlichen und sachlichen Geltungsbereichs des HSchG und der datenschutzrechtlichen Bestimmungen des § 8 HSchG über die Voraussetzungen der Zulässigkeit der Datenverarbeitung notwendig.
Erheblichkeit der Verarbeitung: (Art-29-Datenschutzgruppe, WP 248, 21 iVm Art. 5 Abs. 1 Buchstabe c DSGVO)	Die Verarbeitung der Daten ist erheblich, da sie notwendige Voraussetzung zur Erfüllung der Zwecke des HSchG (§ 1 HSchG) ist. Die Regelung der Datenverarbeitung im HSchG ist erforderlich zur Umsetzung der unionsrechtlichen Vorschrift der Richtlinie 2019/1937/EU zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden.
Beschränktheit der Verarbeitung auf das notwendige Maß: (Art-29-Datenschutzgruppe, WP 248, 21 iVm Art. 5 Abs. 1 Buchstabe c DSGVO)	Die Verarbeitung ist auf das erforderliche Maß beschränkt, weil die bereitgestellten Daten Dritten (Art. 4 Nr. 10 DSGVO) nur zur weiteren Ermittlung oder Einleitung eines Verfahrens zur Kenntnis gebracht werden dürfen (§ 8 Abs. 5 HSchG). Personenbezogene Daten, die für die Bearbeitung eines Hinweises nicht benötigt werden, dürfen nicht erhoben werden bzw. sind unverzüglich zu löschen, falls sie unbeabsichtigt erhoben wurden (§ 8 Abs. 8 HSchG).
Speicherbegrenzung: (Art-29-Datenschutzgruppe, WP 248, 21 iVm Art. 5 Abs. 1 Buchstabe e DSGVO)	Die Speicherdauer ist mit dreißig Jahren ab letztmaliger Verarbeitung oder Übermittlung der personenbezogenen Daten bzw. darüber hinaus mit dem Abschluss eines verwaltungsbehördlichen oder gerichtlichen Verfahrens begrenzt (§ 8 Abs. 9 HSchG). Nach Entfall der Aufbewahrungspflicht sind personenbezogene Daten zu löschen. Protokolldaten sind ab ihrer letztmaligen Verarbeitung oder Übermittlung bis drei Jahre nach Entfall der Pflicht zur Aufbewahrung personenbezogener Daten aufzubewahren (§ 8 Abs. 10 HSchG).
Generelle Information der betroffenen Personen: (Art-29-Datenschutzgruppe, WP 248, 21 iVm Art. 12 DSGVO)	Wie in der unmittelbar folgenden Zeile ausgeführt wird, ist, wenn die Zwecke des HSchG erreicht werden sollen, eine Information der betroffenen Person nur in gesetzlich eingeschränktem Umfang möglich. Eine Information betroffener Personen ist vorgesehen: – in Einzelauskünften entsprechend § 8 Abs. 7 letzter Unterabsatz HSchG, dass Betroffenenrechte auf der Grundlage des Art. 23 DSGVO ausgeschlossen sind; – in der generellen Information entsprechend § 10 Abs. 2 Z 3 HSchG auf den Websites der externen Stellen.
Information der betroffenen Personen bei Erhebung: (Art-29-Datenschutzgruppe, WP 248, 21 iVm Art. 13 DSGVO)	Die Identität von Personen, die von einem Hinweis und daher von einer Verarbeitung ihrer personenbezogenen Daten betroffen sind, ist vor allem unter dem Gesichtspunkt zu schützen, dass sich Hinweise als falsch herausstellen können. Im Regelungszusammenhang besteht jedoch ein Spannungsverhältnis zwischen den Rechten der von Hinweisen betroffenen Personen einerseits und der Gefahr andererseits, die für Hinweisgeberinnen und Hinweisgeber und eine wirksame Verfolgung ihres Hinweises bei einer Bekanntgabe ihrer Daten entstünde. Die Verarbeitung personenbezogener Daten im Rahmen des HSchG muss im Interesse der Ermittlung und Verfolgung der in einem Hinweis vorgeworfenen Rechtsverletzung und zum Schutz der Hinweisgeberinnen und Hinweisgeber
Information der betroffenen Personen, wenn die Daten nicht bei ihnen erhoben werden: (Art-29-Datenschutzgruppe, WP 248, 21 iVm Art. 14 DSGVO)	
Auskunftsrecht der betroffenen Personen: (Art-29-Datenschutzgruppe, WP 248, 21 iVm Art. 15 DSGVO)	
Recht auf Datenübertragbarkeit: (Art. 20 DSGVO)	

	<p>geregelt werden. Die datenschutzrechtlichen Ansprüche der von Hinweisen betroffenen Person sind im Einklang mit Art. 23 DSGVO und EG (84) und (85) der Richtlinie 2019/1937/EU einzuschränken.</p> <p>In diesem Sinn sieht § 8 Abs. 7 HSchG vor, dass innerhalb des Zeitraums des erforderlichen Hinweisgeberschutzes und soweit es für den Hinweisgeberschutz erforderlich ist, die folgenden datenschutzrechtlichen Ansprüche ausgesetzt sind:</p> <ul style="list-style-type: none"> – das Recht auf Information (§ 43 DSG, Art. 13 und 14 DSGVO), – das Recht auf Auskunft (§ 1 Abs. 3 Z 1 und § 44 DSG, Art. 15 DSGVO), – das Recht auf Berichtigung (§ 1 Abs. 3 Z 2 und § 45 DSG, Art. 16 DSGVO), – das Recht auf Löschung (§ 1 Abs. 3 Z 2 und § 45 DSG, Art. 17 DSGVO), – das Recht auf Einschränkung der Verarbeitung (§ 45 DSG, Art. 18 DSGVO), – das Widerspruchsrecht (Art. 21 DSGVO), – das Recht auf Benachrichtigung von einer Verletzung des Schutzes personenbezogener Daten (§ 56 DSG und Art. 34 DSGVO).
Auftragsverarbeiterinnen und Auftragsverarbeiter: (Art. 28 DSGVO)	Da Art. 35 Abs. 10 DSGVO Datenschutzfolgenabschätzungen auch im Zuge von Gesetzgebungsverfahren zulässt und die konkret zum Einsatz kommenden Auftragsverarbeiterinnen und -verarbeiter 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)	Eine Übermittlung von Daten in Drittländer wird vom Entwurf nicht eingeräumt.
Vorherige Konsultation: (Art. 36 und EG 96 DSGVO)	Eine vorherige Konsultation der Datenschutzbehörde im Einzelfall ist nicht erforderlich, weil die Datenschutzbehörde gemäß Art. 36 Abs. 4 DSGVO durch Einbindung bzw. Konsultation (EG 96 DSGVO) und im Begutachtungsverfahren durch Publikation des Entwurfs auf der Website des Parlaments Gelegenheiten hatte und hat, aktiv an der Gestaltung des vorliegenden Entwurfes mitzuwirken, um die Vereinbarkeit der geplanten Verarbeitungen mit der Datenschutz-Grundverordnung sicherzustellen.
<p>RISIKEN</p> <p><i>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:</i></p>	
Physische, materielle oder immaterielle Schäden: (EG 90 iVm 85 DSGVO)	<p>Diese Risiken sind bei Verarbeitungen im Rahmen des HSchG vorhanden, jedoch durch folgende rechtliche Vorkehrungen eingeschränkt:</p> <ul style="list-style-type: none"> – Art. 25 DSGVO verordnet, dass „auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete technische und organisatorische Maßnahmen“ getroffen werden müssen, um „die Rechte der betroffenen Personen zu schützen“. – Ähnlich ordnet Art. 32 DSGVO an, dass Verantwortliche, Auftragsverarbeiterinnen und

	<p>Auftragsverarbeiter in geeigneten technischen und organisatorischen Maßnahmen unter anderem den Stand der Technik und die Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen berücksichtigen müssen.</p> <ul style="list-style-type: none"> – Die Nichteinhaltung ist mit 10 Millionen Euro sanktioniert (Art. 83 Abs. 4 Buchstabe a DSGVO), sodass von der Strafdrohung eine Eindämmung dieses Risikos zu erwarten ist. – Im Entwurf zum HSchG werden weitere Maßnahmen zur Senkung dieses Risikos für betroffene Personen (von einem Hinweis betroffene Personen sowie Hinweisgeberinnen und Hinweisgeber) vorgeschlagen: <ul style="list-style-type: none"> ▪ Bindung des Schutzes für Informationsweitergaben an objektive und subjektive Voraussetzungen (§ 6 HSchG) ▪ Vorschriften zum Schutz der Vertraulichkeit und der Identität betroffener Personen sowie zur Geheimhaltung (§§ 7, 13 Abs. 3, 17 Abs. 1 HSchG) mit Strafdrohung für die Verletzung dieser Vorschriften (§ 24 Z 1 lit. c HSchG; Geldstrafe bis zu € 21.000,-, im Wiederholungsfall bis zu € 42.000,-) ▪ Einschränkung der Offenlegung der Identität betroffener Personen auf behördliche Verfahren (§ 7 Abs. 3 bis 5 HSchG) ▪ Verpflichtung zur Löschung nicht verhältnismäßiger Daten (§ 8 Abs. 8 HSchG).
<p>Verlust der Kontrolle über personenbezogene Daten: (EG 90 iVm 85 DSGVO)</p>	<p>Eine wesentliche Senkung des Risikos erfolgt durch</p> <ul style="list-style-type: none"> – lückenlose Protokollierung (§ 9 HSchG) – Bestimmungen zum Schutz der Vertraulichkeit und der Identität betroffener Personen sowie zur Geheimhaltung (§§ 7, 13 Abs. 3, 17 Abs. 1 HSchG) mit Strafdrohung für die Verletzung dieser Vorschriften (§ 24 Z 1 lit. c HSchG; Geldstrafe bis zu € 21.000,-, im Wiederholungsfall bis zu € 42.000,-) – strenge Zweckbindung in den datenschutzrechtlichen Regelungen (§8 HSchG), durch den persönlichen und sachlichen Geltungsbereich, aufgrund der objektiven und subjektiven Voraussetzungen des Hinweisgeberschutzes (§ 6 HSchG).
<p>Diskriminierung: (EG 90 iVm 85 DSGVO)</p>	<p>Eine wesentliche Senkung dieses Risikos erfolgt insbesondere durch folgende Regelungen:</p> <ul style="list-style-type: none"> – Art. 25 DSGVO, wonach zum Schutz betroffener Personen geeignete technische und organisatorische Maßnahmen getroffen werden müssen. – Art. 32 DSGVO, wonach Verantwortliche, Auftragsverarbeiterinnen und Auftragsverarbeiter in geeigneten technischen und organisatorischen Maßnahmen unter anderem den Stand der Technik und die Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen berücksichtigen müssen. – Die Nichteinhaltung ist mit 10 Millionen Euro sanktioniert (Art. 83 Abs. 4 Buchstabe a DSGVO), sodass von der Strafdrohung eine Eindämmung dieses Risikos zu erwarten ist.

	<ul style="list-style-type: none"> – Für Hinweisgeberinnen und Hinweisgeber und Personen in ihrem Umkreis als jeweils betroffene Personen sieht § 20, insbesondere § 20 Abs. 2 Z 2 HSchG eine ausdrückliche Bestimmung zur Verhinderung von Diskriminierungen vor. – Für von Hinweisen betroffene Personen soll das Risiko nachteiliger Folgen der Datenverarbeitung durch strenge Zweckbindung in den datenschutzrechtlichen Regelungen (§8 HSchG), durch den persönlichen und sachlichen Geltungsbereich, durch die objektiven und subjektiven Voraussetzungen des Hinweisgeberschutzes (§ 6 HSchG) sowie Strafbarkeit missbräuchlicher Hinweisgebung (§ 24 Z 2 HSchG) eingeschränkt werden.
Identitätsdiebstahl oder -betrug: (EG 90 iVm 85 DSGVO)	<p>Dieses Risiko kann insbesondere durch die unionsrechtliche Sanktionierung (siehe oben: Risiken / Physische, materielle oder immaterielle Schäden) gemindert werden.</p> <p>Eine wesentliche Senkung des Risikos erfolgt insbesondere durch</p> <ul style="list-style-type: none"> – lückenlose Protokollierung (§ 9 HSchG) – Bestimmungen zum Schutz der Vertraulichkeit und der Identität betroffener Personen sowie zur Geheimhaltung (§§ 7, 13 Abs. 3, 17 Abs. 1 HSchG) mit Strafandrohung für die Verletzung dieser Vorschriften (§ 24 Z 1 lit. c HSchG; Geldstrafe bis zu € 21.000,--, im Wiederholungsfall bis zu € 42.000,--) – strenge Zweckbindung in den datenschutzrechtlichen Regelungen (§8 HSchG), durch den persönlichen und sachlichen Geltungsbereich, aufgrund der objektiven und subjektiven Voraussetzungen des Hinweisgeberschutzes (§ 6 HSchG).
Finanzielle Verluste: (EG 90 iVm 85 DSGVO)	<p>Dieses Risiko kann insbesondere durch die unionsrechtliche Sanktionierung (siehe oben: Risiken / Physische, materielle oder immaterielle Schäden) gemindert werden.</p> <p>Für Hinweisgeberinnen und Hinweisgeber und Personen in ihrem Umkreis als jeweils betroffene Personen sieht § 20 HSchG Bestimmungen zur Verhinderung finanziell nachteiliger Auswirkungen vor.</p> <p>Für von Hinweisen betroffene Personen soll das Risiko finanziell nachteiliger Folgen der Datenverarbeitung durch strenge Zweckbindung in den datenschutzrechtlichen Regelungen (§8 HSchG), durch den persönlichen und sachlichen Geltungsbereich, durch die objektiven und subjektiven Voraussetzungen des Hinweisgeberschutzes (§ 6 HSchG) sowie Strafbarkeit missbräuchlicher Hinweisgebung (§ 24 Z 2 HSchG) eingeschränkt werden.</p>
Unbefugte Aufhebung der Pseudonymisierung: (EG 90 iVm 85 DSGVO)	<p>Pseudonymisierung spielt im Entwurf allenfalls eine Rolle bei zugelassenen anonymen Hinweisen und im Rahmen künftiger Berichte und statistischer Erfassung der Hinweisgebung.</p> <p>In diesem Rahmen wird das Risiko minimiert durch die unionsrechtliche Sanktionierung (siehe oben: Risiken / Physische, materielle oder immaterielle Schäden) und den Einsatz bereichsspezifischer Personenkennzeichen (§ 9 E-GovG).</p>
Rufschädigung:	Dieses Risiko wird minimiert durch

(EG 90 iVm 85 DSGVO)	<ul style="list-style-type: none"> – die unionsrechtliche Sanktionierung (siehe oben: Risiken / Physische, materielle oder immaterielle Schäden) – durch Regelungen zu den objektiven und subjektiven Voraussetzungen des Hinweisgeberschutzes (§ 6 HSchG) – durch die Regelungen zum Schutz vor Vergeltungsmaßnahmen (§§ 20 und 23 HSchG) – durch den Straftatbestand missbräuchlicher Hinweisgebung (§ 24 Z 2 HSchG).
Verlust der Vertraulichkeit bei Berufsgeheimnissen: (EG 90 iVm 85 DSGVO)	<p>Dieses Risiko wird minimiert durch</p> <ul style="list-style-type: none"> – die unionsrechtliche Sanktionierung (siehe oben: Risiken / Physische, materielle oder immaterielle Schäden) – strenge Voraussetzungen der Benutzung und Offenlegung von Geschäfts- und anderen Geheimnissen in § 7 Abs. 8 und in § 22 HSchG – durch den Straftatbestand missbräuchlicher Hinweisgebung (§ 24 Z 2 HSchG).
Erhebliche wirtschaftliche oder gesellschaftliche Nachteile: (EG 90 iVm 85 DSGVO)	<p>Dieses Risiko wird minimiert durch</p> <ul style="list-style-type: none"> – die unionsrechtliche Sanktionierung (siehe oben: Risiken / Physische, materielle oder immaterielle Schäden) – Bestimmungen zum Schutz der Vertraulichkeit und der Identität betroffener Personen sowie zur Geheimhaltung (§§ 7, 13 Abs. 3, 17 Abs. 1 HSchG) mit Strafandrohung für die Verletzung dieser Vorschriften (§ 24 Z 1 lit. c HSchG; Geldstrafe bis zu € 21.000,--, im Wiederholungsfall bis zu € 42.000,--) – strenge Zweckbindung in den datenschutzrechtlichen Regelungen (§8 HSchG), durch den persönlichen und sachlichen Geltungsbereich, aufgrund der objektiven und subjektiven Voraussetzungen des Hinweisgeberschutzes (§ 6 HSchG) – durch die Regelungen zum Schutz vor Vergeltungsmaßnahmen (§§ 20 und 23 HSchG) – durch die Straftatbestände des § 24 HSchG.
<p>ABHILFEMASSNAHMEN <i>Als Maßnahmen, Garantien und Verfahren zur Eindämmung von Risiken werden insbesondere in den Erwägungsgründen 28, 78 und 83 DSGVO genannt:</i></p>	
Minimierung der Verarbeitung personenbezogener Daten: (EG 78 DSGVO)	<p>Der Entwurf verankert im Konkreten in mehreren Regelungszusammenhängen den Grundsatz, dass nur Daten verarbeitet werden dürfen, die zur Feststellung und Ahndung einer Rechtsverletzung benötigt werden, und anderenfalls nicht erhoben werden dürfen bzw. zu löschen sind (insbesondere in § 7 Abs. 3 und 5, § 8 Abs. 2 Z 2, Abs. 3 Z 1 sowie Abs. 8 HSchG).</p>
Schnellstmögliche Pseudonymisierung personenbezogener Daten: (EG 28 und 78 DSGVO)	<p>Soweit Pseudonymisierung nach dem Entwurf relevant ist, kann auf die Anwendung des bereichsspezifischen Personenkennzeichens (bPk) gem. § 9 E-GovG verwiesen werden.</p>
Transparenz in Bezug auf die Funktionen und die Verarbeitung personenbezogener Daten: (EG 78 DSGVO)	<p>Durch die Publikation des Gesetzesvorhabens als Bundesgesetz im Bundesgesetzblatt sowie der parlamentarischen Materialien im Zuge des Gesetzgebungsprozesses können die Hintergründe für die zulässige Verarbeitung personenbezogener Daten im Rahmen des Gesetzesvorhabens von der Öffentlichkeit kostenlos nachvollzogen werden.</p>

Überwachung der Verarbeitung personenbezogener Daten durch die betroffenen Personen: (EG 78 DSGVO)	Die betroffenen Personen haben durch Ausübung ihrer Rechte gemäß Kapitel III der DSGVO (Transparente Information, Kommunikation und Modalitäten für die Ausübung der Rechte der betroffenen Person (Art. 12 DSGVO)), soweit diese nicht gem. § 8 Abs. 7 HSchG ausgeschlossen sind, die Möglichkeit, die Verarbeitung ihrer Daten zu überwachen.
Datensicherheitsmaßnahmen: (EG 78 und 83 DSGVO)	Die Nichteinhaltung der Datensicherheitsmaßnahmen gemäß Art. 32 DSGVO ist gemäß Art. 83 Abs. 4 Buchstabe a DSGVO mit Geldbußen bis zu 10 Millionen Euro sanktioniert. 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 Datenschutzfolgenabschätzungen auch im Zuge von Gesetzgebungsverfahren zulässt, ist ein Verweis auf die Einhaltung der Maßnahmen gemäß Art. 32 DSGVO als ausreichend anzusehen.
BERÜCKSICHTIGUNG VON DATENSCHUTZINTERESSEN <i>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:</i>	
Stellungnahme der Datenschutzbehörde: (Art. 36 Abs. 4 DSGVO)	im Begutachtungsverfahren zu berücksichtigen
Stellungnahme des Datenschutzbeauftragten der erlassenden Stelle: (Art. 35 Abs. 2 DSGVO)	im Begutachtungsverfahren zu berücksichtigen
Stellungnahme betroffener Personen: (Art. 35 Abs. 9 DSGVO)	im Begutachtungsverfahren zu berücksichtigen