Amt der Oö. Landesregierung
Direktion Verfassungsdienst
4021 Linz • Landhausplatz 1

Beilage zu Verf-2024-157566/6

www.land-oberoesterreich.gv.at

Stand: 13. Juni 2024

Begutachtungsentwurf

betreffend das

Landesgesetz über den Einsatz moderner Informationstechnologien zur Förderung der digitalen Transformation der Verwaltung

(Oö. Informationstechnologien-Einsatz-Gesetz)

A. Allgemeiner Teil

I. Anlass und Inhalt des Gesetzentwurfs

Neben den Grundsätzen der Sparsamkeit, Wirtschaftlichkeit, Zweckmäßigkeit sowie der Wirkungsorientierung des Verwaltungshandelns und den internen Geschäftsprozessen bestimmen die rechtlichen Rahmenbedingungen die digitale Transformation des Verwaltungshandelns. Digitale Prozesse sind der Grundstein für die digitale Transformation und für transparentes, (teil-)automatisiertes Verwaltungshandeln.

Die Anforderungen, die an eine moderne und serviceorientierte Verwaltung gestellt werden, ergeben sich einerseits aus den Bedürfnissen der Bürgerinnen und Bürger sowie der Unternehmen in ihrem täglichen Umgang mit digitalen Angeboten. Andererseits steht die öffentliche Verwaltung „unter dem Druck, in Qualität und Quantität wachsende Anforderungen mit zunehmend weniger Personal bewerkstelligen zu müssen.“ (vgl. Leitfaden Digitale Verwaltung und Ethik. Praxisleitfaden für KI in der Verwaltung, Version 1.0, 40)

Die zunehmende Automatisierung von Arbeitsschritten wird zur Steigerung von Effizienz und Effektivität bei der Leistungserbringung der Verwaltung führen. Außerdem verändert sich das Arbeitsumfeld, wodurch sich die Verwaltung noch mehr als attraktiver Dienstgeber positionieren kann.

In den kommenden Jahren wird der Bedarf für den Einsatz algorithmisch arbeitender Systeme sowie für Künstliche Intelligenz (KI) bzw. Maschinelles Lernen (ML) weiter zunehmen. Diese Technologien werden auch in der digitalen Transformation der Verwaltung eine Schlüsselrolle spielen. Für die vielfältigen Einsatzmöglichkeiten in der Verwaltung soll mit diesem Gesetz - flankierend zu den verschiedenen Normen auf Unionsebene - ein Handlungsrahmen mit Transparenz und Rechtssicherheit geschaffen werden.

Als wesentliche Punkte dieses Gesetzentwurfs sind anzuführen:
- Definition moderner Informationstechnologien;
- Rechtsgrundlage für die (Weiter-)Verarbeitung von personenbezogenen Daten zu Trainings-, Validierungs- und Testzwecken auch von (Nicht-Hochrisiko-)KI-Systemen zur Förderung verantwortungsvoller KI;
- Rechtsgrundlage für Vollautomatisierung in der Privatwirtschaftsverwaltung inkl. flankierender Maßnahmen für einen (DSGVO- und grund-)rechtskonformen Einsatz algorithmisch arbeitender Systeme.

II. Kompetenzgrundlagen

Die Kompetenz des Landesgesetzgebers ergibt sich aus Art. 15 Abs. 1 B-VG.

III. Finanzielle Auswirkungen auf die Gebietskörperschaften

Durch dieses Landesgesetz werden weder dem Land noch den Gemeinden oder dem Bund gegenüber der derzeitigen Rechtslage (nennenswerte) Mehrkosten erwachsen, wenngleich zu berücksichtigen sein wird, dass das Trainieren und der Betrieb von KI-Systemen in der Regel mit hohen Kosten verbunden sind. Die fortschreitende digitale Transformation der Verwaltung, die Anpassung an sich ständig wandelnde technische Standards und damit der vermehrte Einsatz moderner Informationstechnologien ermöglichen einen zielgerichteteren und nutzbringenderen Einsatz wertvoller Personalressourcen. Mitarbeiterinnen und Mitarbeiter können sich auf komplexe Aufgabenstellungen konzentrieren und bei der Aufgabenbewältigung unterstützt werden. Damit können neue Potenziale eröffnet werden.

Es werden grundsätzlich keine zusätzlichen Leistungsprozesse der Verwaltung geschaffen.

IV. Finanzielle Auswirkungen auf Bürgerinnen und Bürger und auf Unternehmen einschließlich der Auswirkungen auf den Wirtschaftsstandort Oberösterreich

Die in diesem Landesgesetz enthaltenen Regelungen bringen keinerlei finanzielle Belastungen für die Bürgerinnen und Bürger im Allgemeinen und für Wirtschaftstreibende im Besonderen mit sich.

Der vorliegende Gesetzentwurf unterstützt die Digitalisierungsbestrebungen der öffentlichen Verwaltung in Oberösterreich und wirkt sich insofern positiv auf den Wirtschaftsstandort Oberösterreich aus.

V. Verhältnis zu Rechtsvorschriften der Europäischen Union

Diesem Landesgesetz stehen - soweit ersichtlich - keine zwingenden unionsrechtlichen Vorschriften entgegen. Insbesondere die Datenschutz-Grundverordnung (DSGVO) und der Artificial Intelligence Act (AI Act) der Europäischen Union sind maßgeblich für den Umfang und die Ausgestaltung dieses Gesetzes.

Der Kriterien- und Maßnahmenkatalog für ethische KI in der Verwaltung (EKIV) als dialogisches Instrument zur Folgenabschätzung und die Checkliste für KI-Projekte sollten sowohl am Anfang eines Planungs-, Beschaffungs- oder Evaluationsprozesses als auch am Ende zur Unterstützung bei der Folgenabschätzung herangezogen werden (sh. Leitfaden Digitale Verwaltung und Ethik. Praxisleitfaden für KI in der Verwaltung, Version 1.0, 52 ff., zuletzt abgerufen am 23. Mai 2024 unter: https://oeffentlicherdienst.gv.at/wp-content/uploads/2023/11/Leitfaden-Digitale-Verwaltung-Ethik.pdf; ebenda der Entscheidungsbaum zur Verwendung datengetriebener KI-Technologie, 38).

Die DSGVO und auch der AI Act adressieren Anforderungen an den Umgang mit Daten, welche berücksichtigt wurden. Der AI Act soll alle in der Europäischen Union angewandten Systeme der Künstlichen Intelligenz durch private und öffentliche Organisationen regulieren. „Mit Transparenz- und Überwachungsvorgaben, insbesondere für KI-Systeme mit hohem Risiko, soll der Markt für KI geregelt, das Vertrauen in KI gestärkt sowie der Nutzer:innenschutz gewährleistet werden. (…) Der AI Act regelt die Entwicklung und Nutzung von KI-Systemen in der EU, indem er die Regeln für die Markteinführung, die Inbetriebnahme und die Nutzung von KI-Systemen harmonisiert (Leitfaden Digitale Verwaltung und Ethik. Praxisleitfaden für KI in der Verwaltung, Version 1.0, 43 f.).“

Neben den allgemeinen datenschutzrechtlichen Grundsätzen des Art. 5 DSGVO und den Bestimmungen des DSG ist für das gegenständliche Gesetz insbesondere auf Art. 22 DSGVO hinzuweisen bzw. auf die Ausführungen zu § 4 verweisen.

Die DSGVO verfolgt bei der Frage, ob eine Datenschutz-Folgenabschätzung (DSFA) notwendig ist, einen risikobasierten Ansatz. Wenn ein Verarbeitungsvorgang voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat, ist gemäß Art. 35 DSGVO eine DSFA

durchzuführen. Bei der Bewertung des Risikos soll berücksichtigt werden, auf welche Art, in welchem Umfang, unter welchen Umständen und zu welchen Zwecken die Verarbeitung erfolgt. Im Art. 35 Abs. 3 DSGVO finden sich beispielhaft genannte Verarbeitungsvorgänge, die jedenfalls einer DSFA bedürfen. Weiters hat die österreichische Datenschutzbehörde Verordnungen erlassen, die regeln, wann jedenfalls eine DSFA durchzuführen ist (Verordnung der Datenschutzbehörde über Verarbeitungsvorgänge, für die eine Datenschutz-Folgenabschätzung durchzuführen ist (DSFA-V)) bzw. wann keine DSFA durchzuführen ist (Verordnung der Datenschutzbehörde über die Ausnahmen von der Datenschutz-Folgenabschätzung (DSFA-AV)). Gegenständlich ist hinsichtlich der automatisierten Entscheidungsfindung insbesondere auf Art. 35 Abs. 3 lit. a DSGVO und § 2 Abs. 2 Z 1, 2 und 4 DSFA-V hinzuweisen. Eine DSFA kann auch auf abstrakter Ebene durchgeführt werden (vgl. Erwägungsgrund 92 DSGVO und Art. 35 Abs. 10 DSGVO).

Nach Art. 35 Abs. 1 letzter Satz DSGVO besteht zudem die Möglichkeit für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohen Risiken eine einzige Abschätzung vorzunehmen.

Für den Anwendungsbereich des Gesetzes wird nachfolgende DSFA durchgeführt (für spezielle Verarbeitungsvorgänge wäre ggf. im Einzelfall zu prüfen, ob gesondert eine DSFA durchzuführen ist):

Datenschutz-Folgenabschätzung „Automatisierte Entscheidungsfindung“	
Systemische Beschreibung der beabsichtigten Verarbeitungsvorgänge	
Bezeichnung der Verarbeitungstätigkeit	Automatisierte Entscheidung bei Leistungen als Träger von Privatrechten
Verarbeitungstätigkeit	Automatisierte Entscheidung in der Privatwirtschaftsverwaltung, insbesondere zum Steigern der Effizienz der Verwaltung beim Vorbereiten und Durchführen von Leistungsgewährungen (zB Förderungen), etwa beim Feststellen des Vorliegens der Voraussetzungen und der Höhe einer Leistung, Sicherstellen einer hohen Datenqualität, Feststellen von Kostenersatzpflichten und Kontrollieren der Rechtmäßigkeit des Leistungsbezugs.
Zweck der Verarbeitung	Die Verarbeitung verfolgt insbesondere den Zweck, die Voraussetzungen für die Leistungsgewährung gemäß der jeweiligen (zB Förderungs-)Richtlinien festzustellen, die Antragstellerinnen und Antragsteller über die Erledigung des Anbringens (Antrag, Eingabe, Begehren, Ansuchen) zu verständigen und ggf. (im positiven Fall) die Auszahlung herbeizuführen.
Datenkategorien (Datenarten)	**Antragsdaten der Antragstellenden**, wie insbesondere - **Identitäts-/Personenstandsdaten**: Titel (optional), Namen (Vor- und Familiennamen sowie sonstige Namen), Geschlecht,

	Geburtsdaten (Ort, Datum, Bundesland, wenn im Inland gelegen, und Staat, wenn im Ausland gelegen), Staatsangehörigkeit (bei Fremden bei Bedarf überdies Art, Nummer, Ausstellungsbehörde und Ausstellungsdatum sowie der Staat der Ausstellung des Dokuments), ggf. Sozialversicherungsnummer (in diesem Kontext nicht als Gesundheitsdatum iSd. Art. 9 DSGVO), Familienstand; - **Haushaltsadresse**: Land, PLZ, Ort, Straße, Hausnummer, Tür/Stock/Stiege, Bezirk, Adresscode, Gemeindekennzahl; Wohneinheitsnummer; - **Kontaktdaten**: E-Mail-Adressen, Telefonnummern; - **Bankverbindung**: IBAN/BIC, Kontoinhaber; - **finanzielle/wirtschaftliche Daten** (uU je nach Richtlinie auch allfälliger Haushaltsangehöriger): Jahresbruttoeinkommen, Grundlage für Lebensunterhaltsbestreitung; - **uU je nach Richtlinie auch allfällige Haushaltsangehörige**: Namen, Geburtsdaten. **Ggf. Abfrageergebnisse (bei entsprechender Legitimation zur Abfrage)**, wie insbesondere - Zentrales Melderegister: (im selben Haushalt) gemeldete Personen mit Namen; Geburtsdaten; „Gemeldet-Ab"-Datum; bereichsspezifische Personenkennzeichen (bPK) Transparenzdatenbank/TDB, Amtliche Statistik/AS, Zentrales Rechnungswesen/HR; Wohneinheitsnummer; - Transparenzdatenbank: TDB-Datenverfügbarkeit je Person, EK-Jahr, Jahresbruttoeinkommen je Haushaltsmitglied. Betreffend bPK wird auf § 9 E-GovG sowie die E-Government-Bereichsabgrenzungsverordnung verwiesen.
Dauer der Verarbeitung (Speicherung)	Die Aufbewahrungsdauer der einzelnen Verarbeitungsvorgänge ergibt sich zum einen aus speziellen gesetzlichen Bestimmungen (zB BAO) bzw. zum anderen aus den jeweiligen Skartierungsvorschriften, wobei das Oö. Archivgesetz zu beachten ist (vgl. insbesondere § 3 Abs. 1 Oö. Archivgesetz).
Ort der Speicherung:	Sichere IT-Infrastruktur, zB des Landes Oberösterreich (die Abt. IT des Amtes der Oö. Landesregierung ist nach ISO 27001 zertifiziert).
Art, Umfang und Inhalt der Verarbeitung	Daten werden nur insoweit erfasst, als diese für die Antragstellung, Prüfung, Abwicklung und ggf. Auszahlung notwendig sind, zB: - Eindeutige Identifikation der Person, ihres Hauptwohnsitzes und ggf. allfälliger Haushaltsangehörigen, um sicherstellen zu

	können, dass nur die berechtigten Personen eine positive Entscheidung erhalten). - Prüfung des Einkommens, um sicherzustellen, dass nur Personen/Haushalte, deren Einkommen jenen in der Richtlinie/Norm festgelegten Richtsätzen entspricht, positiv entschieden werden. - Kontodaten werden benötigt, um eine direkte Überweisung auf das Konto einer anspruchsberechtigten Person durchführen zu können. Nach § 15b Oö. Antidiskriminierungsgesetz sind entsprechende Maßnahmen zur Barrierefreiheit (Leitkriterien Wahrnehmbarkeit, Bedienbarkeit, Verständlichkeit und Robustheit) und damit zur Benutzerfreundlichkeit zu treffen.
Beschreibung der Verarbeitung	1. Aufruf des Formulars (zB Homepage des Landes OÖ) 2. Befüllen des Formulars, wie zB - Eingabe der obigen Daten durch die antragstellende Person/automatisierte Abfrage der erforderlichen Daten bei entsprechender Rechtsgrundlage; - Bestätigung, dass antragstellende(n) Person(en) tatsächlich antragsberechtigt ist (sind); - Zustimmung, dass die Entscheidung nach Maßgabe der (Förderungs-)Richtlinien getroffen wird (dies ist keine Einwilligung zur Datenverarbeitung iSd. Art. 6 Abs. 1 lit. a iVm. Art. 7 DSGVO, sondern ein Akzeptieren der Richtlinien); - Auswahl, ob eine Zusammenfassung der Antragsdaten und weiterer Schriftverkehr über E-Mail erfolgen soll und Eingabe der E-Mail-Adresse (ggf. auch ohne double-opt-in); - Kontrolle der Richtigkeit der angegebenen Daten und Absenden des Formulars mit dem Button „Senden“. 3. Die Ermittlung der Daten erfolgt insbesondere durch - automatisierte Registerabfragen bei entsprechender Grundlage; - manuelle Eingaben berechtigter Personen im Einzelfall. Gemäß definierter Prüfautomatismen nach Maßgabe der jeweiligen Richtlinien werden die Anträge entweder automatisch genehmigt oder abgelehnt; darüber werden die Antragstellenden automatisiert verständigt. Sofern eine Datenklärung notwendig ist, werden die Anbringen von natürlichen Personen gesichtet, um ggf. Datenkorrekturen oder notwendige Ergänzungen vorzunehmen.

	Eine Ablehnung kann - je nach Richtlinie - etwa insbesondere dann erfolgen, wenn - die antragstellende Person bzw. die Haushaltsangehörigen im Zentralen Melderegister nicht identifizierbar sind; - abgefragte Daten nicht mit den Antragsdaten übereinstimmen; - Haushalt bzw. Hauptwohnsitzadresse nicht in Oberösterreich liegen; - Einkommen über den festgelegten Richtsätzen liegen; - für die antragstellende Person bzw. die Haushaltsangehörigen bereits ein Anbringen gestellt wurde bzw. bereits genehmigt wurde.
Umfang der Verarbeitung	Die Datenverarbeitung könnte je nach Richtlinie einen großen Teil der Bevölkerung in Oberösterreich betreffen. Voraussetzung werden idR der Hauptwohnsitz in Oberösterreich sein, ggf. werden Einkommensgrenzen definiert (zB für Einpersonen- und/oder Mehrpersonenhaushalt), ein Anbringen wird idR nur einmal pro Person/Haushalt möglich sein, das Erfüllen aller Kriterien und keine Zugehörigkeit nicht-förderberechtigter Personengruppen.
Angemessenheit der automatisierten Verarbeitung	Hierzu wird auf die im § 4 vorgesehenen Maßnahmen iSd. Art. 22 Abs. 2 lit. b DSGVO und die Ausführungen zu § 4 verwiesen. Zudem bestehen besondere Informationspflichten nach Art. 13 Abs. 2 lit. f und Art. 14 Abs. 2 lit. g DSGVO. Die betroffene Person ist zu informieren über: - das Bestehen einer automatisierten Entscheidungsfindung, - die damit verbundene Logik zur Nachvollziehbarkeit der Entscheidung sowie - die Bedeutung und die beabsichtigten Folgen für die betroffene Person.
Rechtmäßigkeit der Datenverarbeitung	
Rechtsgrundlagen	Die Verarbeitung der Daten erfolgt auf Grundlage und nach Maßgabe des jeweiligen Materienrechts oder nach Maßgabe der jeweiligen Fördervereinbarung und den (Förderungs-)Richtlinien. Die Speicherung der Daten ergibt sich zT direkt aus gesetzlichen Bestimmungen (zB Haushaltsrecht bzw. BAO). Zudem wird auch von der Judikatur anerkannt, dass die Dokumentation über staatliches Handeln in Aktenform für einen Rechtsstaat unerlässlich ist. So ist es anerkannt, „dass Akten während einer gewissen mehrere Jahre dauernden Skartierungsfrist jedenfalls aufzubewahren sind, und erst dann darüber entschieden wird, ob sie vernichtet oder infolge Archivwürdigkeit dem Archiv zur dauernden

	Aufbewahrung übergeben werden.“ Diese Aufbewahrung der Dokumentation über staatliches Handeln zum Zweck der Nachprüfbarkeit ist als vom „Zweck der Ermittlung“ mitgetragen anzusehen (vgl. DSK 20.01.2010, K121.553/0003-DSK/2010). Die Annahme einer Pflicht zur sofortigen Vernichtung der Verfahrensdokumentation nach Verfahrensbeendigung würde demgegenüber die Gefahr der Förderung von Rechtswillkür und Korruption in sich bergen (BVwG 31.08.2017, W214 2152086-1; VfGH 16.12.2009, B 298/09; 16.03.2001, B 1117/99 Anlassfall zu 16.03.2001, G94/00; VwGH 27.10.2014, Ra 2014/04/0032; 18.03.2015, Ra 2015/04/0008).
Risikoanalyse	
Risiko: Unrichtige Entscheidungen auf Grund der automatisierten Entscheidungsfindung	
Mögliches Risiko und Bedrohungsquelle	Es besteht die Gefahr falscher Entscheidungen (bspw. Ablehnung trotz Erfüllen der Voraussetzungen).
Vorläufige Bewertung von Risiko und dessen Eintrittswahrscheinlichkeit	Eingeschränkt Siehe dazu die im § 4 Abs. 3 vorgesehenen Maßnahmen zur Sicherstellung einer richtigen Entscheidungsfindung.
Folgen eines möglichen Eintritts des Risikos	Wesentlich Durch unrichtige Entscheidungsfindungen besteht die Möglichkeit, dass antragstellende Personen - obwohl sie grundsätzlich die Voraussetzungen erfüllen - eine Ablehnung erhalten (oder umgekehrt).
Abhilfemaßnahmen zur Minderung des Risikos	Risikominimierung Nach § 4 Abs. 2 sind automatisierte Entscheidungen zu begründen und entsprechend zu kennzeichnen. Nach § 4 Abs. 3 sind zudem entsprechende Maßnahmen zu treffen, wie etwa die Implementierung wirksamer Kontrollen. Zudem können betroffene Personen mit dem Verantwortlichen Kontakt aufnehmen. Dafür gibt es bereits jetzt etablierte Prozesse (zB Beschwerdemanagement; vgl. zum Rechtsweg RIS-Justiz RS0018989). Siehe dazu im Detail § 4 samt Ausführungen.
Gesamtrisiko	Mittel
Klassifizierung Restrisiko	Eingeschränkt
Risiko: Echtheit und Glaubwürdigkeit von Daten kann nicht nachvollzogen werden	
Mögliches Risiko und Bedrohungsquelle	Sofern keine Identifikation im Vorfeld stattfindet, ist potentiell nicht erkennbar, welcher Person ein bestimmter Datensatz zuordenbar ist. Ebenso besteht das Risiko einer absichtlichen Falscheingabe

	von Daten, zB Kontoverbindungen und/oder Kontaktdaten, durch Personen.
Vorläufige Bewertung von Risiko und dessen Eintrittswahrscheinlichkeit	Vernachlässigbar Es ist nahezu ausgeschlossen, dass ein Datensatz einer bestimmten Person nicht zugeordnet werden kann. Mit den Daten und ggf. Registerabfragen sind die betroffenen Personen eindeutig identifizierbar. (Bewusst) falsche Antragsdaten werden idR zur Ablehnung führen.
Folgen eines möglichen Eintritts des Risikos	Vernachlässigbar (Bewusst) falsche Antragsdaten würden die Identifikation einer bestimmten Person unmöglich machen, dann können auch keine Nachteile entstehen. Sollte dennoch zB ein genehmigter Zuschuss auf ein Konto einer nicht-berechtigten Person überwiesen werden, besteht die Möglichkeit einer Rückabwicklung.
Abhilfemaßnahmen zur Minderung des Risikos	Risikominimierung Siehe Ablauf.
Gesamtrisiko	Gering
Klassifizierung Restrisiko	Vernachlässigbar

Ergebnis

Die Analyse der wichtigsten Schutzziele der DSGVO hat ergeben, dass nur ein geringes bis mittleres Gesamtrisiko besteht. Trotz der Tatsache, dass (uU auch eine Vielzahl) an personenbezogenen Daten mittels automatisierter Entscheidungsfindung verarbeitet werden, ist auf Grund der IT-Infrastruktur, der datenschutzfreundlichen Gestaltung der jeweiligen Anwendung sowie der technischen und organisatorischen Maßnahmen das **Gesamtrisiko als akzeptabel** zu bewerten. Dies insbesondere auch deshalb, weil die mit der Verarbeitung verbundenen Gefahren durch die beschriebenen Maßnahmen beherrscht werden. Auf Grund der gesetzten Maßnahmen des Verantwortlichen werden die identifizierten bzw. verbleibenden Risiken für die betroffenen Personen angemessen reduziert, sodass insgesamt kein hohes Risiko vorliegt. Die Notwendigkeit und Verhältnismäßigkeit der Datenverarbeitungsprozesse werden auf Basis der entsprechenden systematischen Analyse in Verbindung mit den Rechtsgrundlagen und unter Berücksichtigung aller technischen und organisatorischen Maßnahmen als gegeben erachtet.

Die Risiken der geplanten Verarbeitungsprozesse werden ausreichend eingedämmt und der Schutz personenbezogener Daten wird sichergestellt. Die Einhaltung der datenschutzrechtlichen Anforderungen und Bestimmungen wird gewährleistet.

VI. Auswirkungen auf die verschiedenen Gruppen der Gesellschaft, insbesondere auf Frauen und Männer

Die Texte der vorliegenden Gesetzesnovelle wurden geschlechtergerecht formuliert.

Die in diesem Landesgesetz enthaltenen Regelungen haben - soweit ersichtlich - weder direkt noch indirekt unterschiedliche Auswirkungen auf die verschiedenen Gruppen der Gesellschaft, insbesondere auf Frauen und Männer.

Hinsichtlich § 3 betreffend Entwicklung und Training von (Nicht-Hochrisiko-)KI-Systemen ist jedoch zu bedenken, dass KI-Systeme trotz ihrer Effizienz nicht frei von Fehlern sind. Probleme sind die möglichen Bias und die Diskriminierung, die potentiell auftreten können. „Wenn KI-Algorithmen auf unzureichenden oder voreingenommenen Daten trainiert werden, können sie Vorurteile entwickeln und Entscheidungen treffen, die bestimmte Gruppen benachteiligen. Dies kann zu ethischen und sozialen Problemen führen und erfordert eine umfassende Prüfung und Überwachung der KI-Anwendungen.“ (*Pollirer*, Checkliste Künstliche Intelligenz und Datenschutz, Dako 2023/44)

Um diesen Problemen gegenzusteuern, muss auf eine sorgfältige Datenauswahl und -bereinigung geachtet werden. Daher müssen die Trainings-, Validierungs- und Testdaten hinreichend relevant, repräsentativ, nicht-diskriminierend, integer, objektiv und so weit wie möglich fehlerfrei und vollständig sein. Ebenso wichtig ist die Integration ethischer Richtlinien in den Entwicklungsprozess von KI-Systemen, um sicherzustellen, dass diese Technologien fair und gerecht bleiben. Nur durch die Schaffung transparenter, ethischer Standards und die fortlaufende Überprüfung und Anpassung können Bias und Diskriminierung hintangehalten werden.

Zudem soll die Funktionsweise der eingesetzten modernen Technologien nachvollziehbar sein (Ergebnistransparenz). Bei regelbasierten Systemen ist die Entscheidungsfindung, dh. die involvierte Logik, die zum Ergebnis geführt hat, transparent darstellbar. Nach der Judikatur des EuGH ist beim Einsatz von (teil-)autonomen Entscheidungssystemen bzw. (teilweise) automatisierten Entscheidungsverfahren zu beachten, dass nachprüfende Organe selbständig die Zuverlässigkeit bzw. wissenschaftliche Solidität eingesetzter technischer Systeme verifizieren können müssen. Das System müsste also offenlegen, wie (dh. auch auf Grund welcher Beweiswürdigung) es zu der Annahme des Sachverhalts und der getroffenen Entscheidung gekommen ist, sprich welche „Denk-“ bzw. Rechenprozesse ausschlaggebend waren (vgl. *Klaushofer*, Die österreichischen Verwaltungsgerichte im Lichte der Europäischen Menschenrechtskonvention - digitale Herausforderungen, ZVG 2020, 32 mwN, insbesondere betreffend EuGH 07.11.2018, verb RS C-293/17 und C-294/17; vgl. idS auch *Gantner/Gärnter*, Code Is Interpretation - Legal Explainability und Software-Entwicklung, in *Schweighofer/Kummer/ Saarenpää*, IRIS 2019, 54 ff., welche anhand des Arbeitszeitrechners für die AK-Wien die Abbildung der Begründungsstrukturen der im Code interpretierten Rechtsnormen [zB mittels dynamischer Erklärungstexte zur jeweiligen Berechnung] darlegen).

Weiters sollte beim Einsatz von KI-Systemen (auch außerhalb des AI Act) ein Selbst-Assessment angestrebt werden (z.B. High Level Expert Group on AI, Bewertungsliste für Vertrauenswürdige KI abrufbar unter: https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai, zuletzt abgerufen am 23.05.2024). „Ein solches Assessment für zuverlässige Künstliche Intelligenz ist ein wesentliches Instrument, um sicherzustellen, dass KI-Systeme ethisch, fair und vertrauenswürdig eingesetzt werden. Die Checkliste dient dazu, im Einklang mit Prinzipien und Richtlinien vorzugehen sowie sicherzustellen, dass KI-Anwendungen die Werte der Gesellschaft respektieren und den Menschen dienen." (*Gesek/Hackl,* Stand und Ausblick von Justizanwendungen mit KI-Technologie zur Unterstützung der Rechtsprechung, RZ 2024/13)

„Um Sicherheit für die Nutzung bestimmter Anwendungen oder Datensätze zu erhalten, empfiehlt sich die Erarbeitung bzw. Verwendung von Zertifizierungen. Diese liegen, für verschiedene Zwecke, beispielsweise vom TÜV Austria, dem IEEE und der ISO bereits vor (IEEE SA 2021; TÜV Austria, Institute for Machine Learning 2021; ISO 2022). Andere Tools, wie beispielsweise im Fall der Zertifizierung von Datensätzen, data.nutrition oder data.hazards, sind in Entstehung begriffen." (Leitfaden Digitale Verwaltung und Ethik. Praxisleitfaden für KI in der Verwaltung, Version 1.0, 65)

VII. Auswirkungen in umweltpolitischer Hinsicht, insbesondere Klimaverträglichkeit

Die in diesem Landesgesetz enthaltenen Regelungen weisen keinerlei umweltpolitische Relevanz auf.

VIII. Besonderheiten des Gesetzgebungsverfahrens

Der vorliegende Gesetzentwurf enthält keine Verfassungsbestimmungen.

Eine Mitwirkung von Bundesorganen im Sinn des Art. 97 Abs. 2 B-VG ist im vorliegenden Gesetzentwurf nicht vorgesehen.

B. Besonderer Teil

Zu § 1:

Dieses Gesetz schafft Rechtssicherheit für den Einsatz moderner Informationstechnologien und dient der Fortentwicklung der digitalen Transformation der öffentlichen Verwaltung und der Stärkung des Wirtschaftsstandorts Oberösterreich. Eine moderne Verwaltung braucht innovative, digitale Lösungen, dazu bedarf es einer end-to-end-Digitalisierung und (Teil-)Automation von Verwaltungsprozessen. Dadurch kann nicht nur die Effizienz und Effektivität staatlichen Handelns verbessert werden, sondern es ergeben sich auch neue Potenziale, die Transparenz staatlicher

Verfahren und Entscheidungsprozesse gegenüber Bürgerinnen und Bürgern sowie Unternehmen zu erhöhen.

Zu § 2 Z 3:

Diese Bestimmung definiert den Begriff „moderne Informationstechnologien“. Moderne Informationstechnologien stellen einen zentralen Baustein der digitalen Transformation einer serviceorientierten Verwaltung dar, auch eine vollständig automatisierte Bearbeitung und Entscheidung ist - nach Maßgabe der geltenden Bestimmungen - möglich.

Es handelt sich um einen Oberbegriff für unterschiedliche Systeme: Dazu zählen nicht nur spezielle Systeme, die sich unter Einsatz künstlicher neuronaler Netze und maschineller Lernverfahren und ohne aktiven Eingriff weiterentwickeln können („KI-Systeme“). Auch jene algorithmisch arbeitenden Systeme, die auf Grundlage einer sich nicht verändernden Datengrundlage Daten verarbeiten und gegebenenfalls Entscheidungen treffen können („traditionelle Algorithmen“), sind unter dem Oberbegriff zu subsumieren.

Zu § 3:

Zu Abs. 1:
Werden personenbezogene Daten verarbeitet, muss nicht nur für die Datenverarbeitung im konkreten Einzelfall, sondern auch für die Entwicklung von modernen Informationstechnologien sowie für deren Training bzw. Optimierung die datenschutzrechtliche Zulässigkeit gegeben sein.

In Entsprechung der datenschutzrechtlichen Grundsätze sind die Daten zu anonymisieren oder, falls eine Anonymisierung nicht möglich ist, zu pseudonymisieren, sofern der Zweck nicht beeinträchtigt wird und gleichwertige Ergebnisse/effektives Training nicht oder nur mit unverhältnismäßigem Aufwand auf andere Weise wirksam erzielt werden können. Damit wird auch für die Anonymisierung bzw. Pseudonymisierung der Trainings-, Validierungs- und Testdaten(-sätze) als Verarbeitungsvorgang iSd. Art. 4 Z 2 DSGVO eine Rechtsgrundlage geschaffen.

Mit § 3 wird - in Anlehnung an die Legitimation der Weiterverarbeitung nach § 7 Abs. 1 DSG - eine ausdrückliche Rechtsgrundlage für die Verarbeitung von personenbezogenen Daten durch Verantwortliche des öffentlichen Bereichs für die Entwicklung moderner Technologien sowie zum Trainieren, Validieren und Testen geschaffen, wenngleich gesonderte materiengesetzliche Regelungen zB zur Verarbeitung von Daten zum Zweck der wissenschaftlichen Forschung als leges speciales vorgehen. Eine über § 7 DSG hinausgehende Regelung ist erforderlich, weil die Verarbeitung in der Trainingsphase zwar grundsätzlich auf § 7 Abs. 1 Z 2 DSG gestützt werden kann, da die Ausnahmen vom Zweckbindungsgrundsatz für wissenschaftliche Forschungszwecke grundsätzlich weit interpretiert werden, allerdings besteht hier die Problematik des uU fließenden Übergangs von Entwicklung und Anwendung (vgl. *Dürager*, Künstliche Intelligenz - eine besondere

Art des Profiling nach der DSGVO, Jahrbuch Datenschutzrecht 2019, 381 ff.; *Wirthumer,* Aspekte der (Teil-)Automatisierbarkeit des Verwaltungsverfahrens und der oberösterreichische Weg zum Digitalen Amt, in Braun-Binder/Bußjäger/Eller (Hrsg.), Auswirkung der Digitalisierung auf die Zuordnung und Erlassung behördlicher Entscheidungen (2021) 99 f.).

Die Qualität der Ergebnisse der Systeme steigt mit der Quantität an brauchbaren, qualitativen Trainings-, Validierungs- und Testdaten(-sätzen). Für Entscheidungssysteme ist hier etwa an Rechtstexte, (anonymisierte) Entscheidungen und Erlässe zu denken. Im digitalen Rechtsinformationssystem des Bundes (RIS) sind jedoch die erstinstanzlichen Entscheidungen von den Behörden nicht veröffentlicht. Die Weiterverarbeitung von in internen Erledigungen verarbeiteten Daten (zB Bescheide in elektronischen Aktenverwaltungssystemen zum Training von KI-Systemen) bedarf nach der DSGVO einer Rechtsgrundlage.

Ist der Zweck der Weiterverarbeitung mit dem Zweck, für den die personenbezogenen Daten ursprünglich erhoben wurden, nicht vereinbar, muss auf die Verarbeitung mindestens einer der in Art. 6 Abs. 4 DSGVO genannten Gründe zutreffen. Liegen diese Kriterien nicht vor und kann die Weiterverarbeitung nicht auf die Einwilligung der betroffenen Personen gestützt werden, bedarf es für die Zulässigkeit der Weiterverarbeitung iSd. Art. 5 Abs. 1 lit. b, Art. 6 Abs. 1 lit. a und Art. 6 Abs. 4 DSGVO einer Rechtsvorschrift der Union oder der Mitgliedstaaten, die in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme zum Schutz der im Art. 23 Abs. 1 DSGVO genannten Ziele darstellt. Mit § 3 wird eine notwendige und verhältnismäßige Maßnahme für wichtige Ziele des allgemeinen öffentlichen Interesses geschaffen. Insbesondere sind es wichtige wirtschaftliche oder finanzielle Interessen im Sinn des Art. 23 Abs. 1 lit. e DSGVO, weil damit ein Schritt gesetzt wird, die Verwaltungsrechtspflege bei gleichzeitig steigender Komplexität des Vollzugs sicherzustellen, indem

- repetitive und datenintensive Vorgänge sukzessive beschleunigt und effizienter werden,
- der Wirtschaftsstandort durch schnellere Verfahren gestärkt wird und
- dem (auf Grund des durch den demografischen Wandel bedingten Rückgangs der erwerbstätigen Bevölkerung) zu erwartenden Personalmangel entgegengewirkt wird.

Auch der AI Act erkennt darin ein erhebliches öffentliches Interesse, da damit die Effizienz und Qualität der öffentlichen Verwaltung und öffentlicher Dienste erhöht wird (vgl. etwa Art. 59 Abs. 1 lit. a lit. v AI Act; EWG 63, 140). Der AI Act erlaubt überdies auch das Trainieren, Validieren und Testen von Hochrisiko-KI-Systemen mit personenbezogenen Daten (vgl. Art. 10 Abs. 2 lit. b und Abs. 5 AI Act; EWG 63, 67, 69 f. AI Act).

Zu Abs. 2:

Hinsichtlich der Auswahl der Daten ist darauf zu achten, dass diese hinreichend relevant, repräsentativ, nicht-diskriminierend, integer, objektiv und so weit wie möglich fehlerfrei und vollständig sind. Im Detail kann insbesondere auf die Ausführungen von *Mayrhofer/Parycek*, Digitalisierung des Rechts - Herausforderungen und Voraussetzungen, 21. ÖJT Band IV/1, 11, 36, 84 f., 120 verwiesen werden. Die Europäische Kommission (COM (2020) 65, WEISSBUCH Zur Künstlichen Intelligenz - ein europäisches Konzept für Exzellenz und Vertrauen) stellt Anforderungen

zB an Trainingsdaten dar und beschreibt, wie diese und andere Anforderungen (zB Robustheit und Genauigkeit, menschliche Aufsicht) in einem entsprechenden Rechtsrahmen spezifiziert werden sollten (vgl. weiters *Klaushofer*, Die österreichischen Verwaltungsgerichte im Lichte der Europäischen Menschenrechtskonvention - digitale Herausforderungen, ZVG 2020, 28 f.*; Österreichischer Rat für Robotik und Künstliche Intelligenz*, White Paper - Die Zukunft Österreichs mit Robotik und Künstlicher Intelligenz positiv gestalten, 45 ff. (November 2018); *Hochrangige Expertengruppe für Künstliche Intelligenz*, Ethik-Leitlinien für eine vertrauenswürdige KI, Rz. 73, 80, 101 (08.04.2019); *Ebenhoch/Gantner*, Das Recht in der KI-Falle, in *Schweighofer/Kummer/Saarenpää*, IRIS 2019, 467 f.; Österreichischer Forschungs- und Technologiebericht 2020, III-139 BlgNR 27. GP 02 Hauptdokument 182).

Zu Abs. 3:

Durch den Einsatz gewisser Informationstechnologien ist mitunter nur der Entscheidungsausgang sichtbar. Da dieser nicht zuletzt von den eingesetzten Trainings-, Validierungs- und Testdaten(-sätzen), sprich der Datenbasis abhängt, ist eine entsprechende Dokumentation vorzunehmen, denn die Datenquellen bzw. Datenerhebungen bilden die Basis für die Datenaus- und -bewertungen. „Systemtransparenz umfasst Informationen zu dem IT-System, den eingesetzten Algorithmen und den verwendeten Daten - sowohl die Trainingsdaten im Fall von maschinell-lernenden Systemen als auch die verarbeiteten Daten für die jeweilige Entscheidung.“ (*Mayrhofer/Parycek*, Digitalisierung des Rechts - Herausforderungen und Voraussetzungen, 21. ÖJT Band IV/1, 12)

Siehe dazu auch die Ausführungen zu § 5.

Zu Abs. 4:

Mit dieser Bestimmung soll sichergestellt werden, dass das Trainieren von modernen Informationstechnologien keine nachteiligen Konsequenzen für Einzelpersonen hat. Personenbezogene Daten werden verantwortungsvoll und ethisch verwendet, wodurch die individuellen Rechte der betroffenen Person gewährleistet werden.

Zu Abs. 5:

Die Dokumentation der Herkunft der Daten, des Erhebungszwecks, des Erhebungskontextes und des Erhebungszeitpunkts, des Datenlieferanten sowie der Gründe, Entwicklungsschritte und Testergebnisse gewährleistet Transparenz und erfüllt die Rechenschaftspflicht. Dadurch können potenzielle Risiken und ethische Bedenken im Zusammenhang mit der Verwendung von Daten für Trainingszwecke identifiziert und adressiert werden. Die Dokumentation trägt auch dazu bei, den Prozess nachvollziehbar zu machen und die Einhaltung rechtlicher Anforderungen sicherzustellen.

Zu Abs. 6:

Damit werden entsprechende Datensicherheitsmaßnahmen iSd. DSG und DSGVO normiert.

Zu Abs. 7:

Die Legaldefinition des für die Verarbeitung Verantwortlichen im Art. 4 Z 7 DSGVO sieht vor, dass Zweck und Mittel einer Verarbeitung nicht nur von einem Verantwortlichen bestimmt werden können, sondern die Entscheidung darüber auch von mehreren Verantwortlichen gemeinsam getroffen werden kann. Art. 26 Abs. 1 DSGVO führt dazu aus: „(…) Legen zwei oder mehr Verantwortliche gemeinsam die Zwecke der und die Mittel zur Verarbeitung fest, so sind sie gemeinsam Verantwortliche (…)".

Die gemeinsame Entwicklung moderner Informationstechnologie stellt eine solche Entscheidung (im Sinn einer gemeinsamen Festlegung) über Zwecke der und Mittel zur Datenverarbeitung durch die jeweils beteiligten Verantwortlichen dar. Bei der gemeinsamen Verarbeitung nach Abs. 1 kann es auch zur wechselseitigen Datenübermittlung kommen bzw. ein gemeinsamer Datenpool entstehen.

Liegt eine gemeinsame Verantwortlichkeit vor, sind die jeweiligen (sich aus der DSGVO ergebenden) Verpflichtungen der gemeinsam Verantwortlichen gemäß Art. 26 Abs. 1 zweiter Satz DSGVO in transparenter Form in einer Vereinbarung festzulegen. Die jeweiligen Verpflichtungen bedürfen aber keiner Vereinbarung, „(…) sofern und soweit die jeweiligen Aufgaben der Verantwortlichen nicht durch Rechtsvorschriften der Union oder der Mitgliedstaaten, denen die Verantwortlichen unterliegen, festgelegt sind. (…)". Von dieser in der DSGVO vorgesehenen Möglichkeit wird hiermit Gebrauch gemacht. Die Anlaufstelle wird den betroffenen Personen auf geeignete Weise (zB Internet, Information nach Art. 13 oder 14 DSGVO) bekanntgegeben.

Zu § 4:

Mit § 4 wird eine Rechtsgrundlage für die automatisierte Entscheidungsfindung durch algorithmisch arbeitende Systeme zur Leistungserbringung in der Privatwirtschaftsverwaltung geschaffen. „Assistenzsysteme" iSv. Systemen, die keine automatisierten Entscheidungen treffen, können auch ohne Regelung eingesetzt werden (zB Fachanwendungen, Textbausteine).

Diese Bestimmung erstreckt sich de lege lata nicht auf Erledigungen iSd. § 18 AVG. Weiters kann eine automatisierte Entscheidung mit KI-Systemen nicht auf dieses Gesetz gestützt werden, hierfür sind die Bestimmungen des AI Act zu beachten (vgl. zB Art. 6 Abs. 2 iVm. Anhang III Z. 5 lit. a AI Act).

§ 4 trägt insbesondere den Anforderungen des Art. 22 DSGVO Rechnung. Demnach soll der einzelne Mensch grundsätzlich nicht zum Objekt ausschließlich maschineller Entscheidungen werden. Ausnahmen von diesem Verbot werden im Art. 22 Abs. 2 DSGVO normiert. Art. 22 Abs. 1 DSGVO ist nicht anwendbar, wenn mittels automatisierter Verarbeitung nur Vorschläge erstellt werden, dh. im Einzelfall ein Mensch die Entscheidung auf der Grundlage einer Empfehlung trifft, die durch ein System automatisiert vorgeschlagen wurde. Ein routinemäßiges Bestätigen durch einen Menschen ohne Einflussnahme auf das Ergebnis der vorgeschlagenen Entscheidung als

„*symbolische Geste*“ ist allerdings nicht ausreichend, wobei die Intensität von „*Plausibilitätschecks*“ uU auch vom Risiko für die betroffenen Personen abhängen wird (vgl. *Wirthumer,* Aspekte der (Teil-) Automatisierbarkeit des Verwaltungsverfahrens und der oberösterreichische Weg zum Digitalen Amt, in Braun-Binder/Bußjäger/Eller (Hrsg.), Auswirkung der Digitalisierung auf die Zuordnung und Erlassung behördlicher Entscheidungen (2021) 108 f.).

Art. 22 Abs. 2 lit. b DSGVO enthält eine fakultative Öffnungsklausel, welche den Mitgliedstaaten ermöglicht, über die Regelung des Art. 22 Abs. 2 lit. a und c DSGVO hinausgehende Zulässigkeitstatbestände für automatisierte Entscheidungen im nationalen Recht zu schaffen. „Damit ermöglicht es Art. 22 Abs. 2 lit. b DSGVO dem europäischen und nationalen Gesetzgeber Rechtsvorschriften vorzusehen, die zur Durchbrechung der „roten Linie“ ermächtigen, allerdings (nur) unter der Voraussetzung, dass „angemessene Maßnahmen“ zur Wahrung der Rechte der betroffenen Personen vorgesehen sind. Man kann nun beklagen, dass diese Ausnahmebestimmung auf Grund ihrer Unbestimmtheit und des Spielraums, der bei der Konkretisierung des Begriffs „angemessene Maßnahmen“ besteht, die Einschränkung des Einsatzes von KI zur Entscheidungsfindung mehr oder weniger aushebelt, oder man sieht darin eine Möglichkeit, neue Entwicklungen im Bereich der KI [Anm.: die automatisierte Entscheidung nach § 4 erfolgt nicht mit KI-Systemen] mit der DSGVO in Einklang bringen zu können. Gerade im Datenschutzrecht sind ähnlichen unbestimmte Rechtsbegriffen keine Seltenheit und somit ist deren (allmähliche) Konkretisierung im Einzelfall durch Gerichte und durch die Fachliteratur alles andere als ungewöhnlich.“ (*Jahnel*, Datenschutzrechtliche Grenzen des Einsatzes von KI-unterstützten Legal Tech Tools, ÖZW 2023, 117)

Die Rechtsvorschriften müssen nach Art. 22 Abs. 2 lit. b DSGVO angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person enthalten. „(…) Damit soll sichergestellt werden, dass die Mitgliedstaaten den Schutzstandard der DSGVO nicht aushöhlen und die Wertungen des Unionsrechts nicht unterlaufen. Geeignet sind nur Erlaubnistatbestände, die konkrete risikobezogene Anforderungen formulieren sowie ergänzende Informations- und Beteiligungsmöglichkeiten für die betroffene Person vorsehen. Welche Garantien der Verordnungsgeber dabei im Einzelnen im Blick gehabt hat, deuten Art. 22 Abs. 3 sowie die EG 71 UAbs. 1 S 4 und S 5 an. Zu den Schutzmaßnahmen können danach insbesondere eine spezifische Unterrichtung der betroffenen Person sowie ein Anspruch auf direktes Eingreifen einer Person, auf Darlegung des eigenen Standpunktes, auf Erläuterung der getroffenen Entscheidung und auf Anfechtung der Entscheidung zählen. Der Normgeber kann aber auch teilweise oder ausschließlich andere geeignete Maßnahmen vorsehen. (…)” (*Scholz* in *Simitis/Hornung/Spiecker,* Datenschutzrecht (2019), Art. 22 DSGVO Rn. 46 f.)

Es ist zu bedenken, dass automatisierte Entscheidungen nach § 4 nur bei Leistungserbringungen in der Privatwirtschaftsverwaltung getroffen werden. Auch hier wird der Gleichheitsgrundsatz beachtet. Bereits jetzt bestehen etablierte Möglichkeiten für die betroffene Person sich an den Verantwortlichen zu wenden, sollte bei gleichen Sachverhalten ohne besondere sachliche, am Förderungszweck ausgerichtete Rechtfertigungsgründe unterschiedlich entschieden werden (vgl.

OGH 26.01.1995, 6 Ob 514/95; RIS-Justiz RS0018989: „Auf die Gewährung einer Subvention besteht im allgemeinen kein Rechtsanspruch. Wenn aber eine Subvention bescheidmäßig oder durch Abschluss eines privatrechtlichen Rechtsgeschäftes zuerkannt wurde, so entsteht ein Rechtsanspruch, der im Fall der bescheidmäßigen Zuerkennung im Weg einer Klage beim Verfassungsgerichtshof gemäß Art 137 B - VG, sonst im Rechtsweg durchgesetzt werden kann."). Liegen nicht alle vorgesehenen Fördervoraussetzungen vor, ist das Nichtgewähren der jeweiligen Förderung sachlich gerechtfertigt. Ist ein Förderprogramm zeitlich befristet und/oder mit einem Rahmenbetrag („Fördertopf") begrenzt, kann die Leistung trotz Erfüllen aller Fördervoraussetzungen grundsätzlich etwa nur gewährt werden, wenn noch ausreichend budgetäre Mittel vorhanden sind.

Eine vollautomatisierte oder autonomisierte Entscheidung im Sinn dieses Gesetzes muss eine Festlegung auf ein bestimmtes Ergebnis zur Folge haben, die eine Wirkung in der Außenwelt erzielt. „Die algorithmische Analyse muss auf geeigneten mathematischen bzw. statistischen Verfahren beruhen, die das Fehlerrisiko minimieren und unzutreffende Daten aufdecken und korrigieren, sowie insbesondere diskriminierende Wirkungen (etwa Preisdiskriminierung) nach Möglichkeit ausschließen. (…) Die Ergebnisse automatisierter Verarbeitungen beruhen (…) nur dann auf fairen und geeigneten Mechanismen, wenn auch die Analysen auf einer inhaltlichen korrekten und aktuellen Datengrundlage aufsetzen. Anderenfalls kann das Verarbeitungsverfahren seinem Wesen nach nicht zu richtigen Ergebnissen gelangen. Der Verantwortliche hat daher technische und organisatorische Maßnahmen zu treffen, welche die Richtigkeit der Datengrundlage prüfen und ggf. korrigieren sowie das Risiko von Fehlern minimieren." *(Paal/Pauly/Martini*, DS-GVO[3] (2021), Art. 22 Rn. 36a und 39e)

Dies geschieht mit dem im § 4 Abs. 3 vorgesehenen Mindestset an (weiteren) angemessenen technischen und organisatorischen Maßnahmen, die nicht zuletzt aus datenschutzrechtlicher Perspektive erforderlich sind (vgl. insbesondere Art. 22, 24 und 32 DSGVO). So wird etwa mit Testszenarien, Simulationen und umfassenden Validierungsverfahren sichergestellt, dass das System zuverlässig, korrekt und angemessen funktioniert. Mit einem wirksamen Kontrollsystem werden die automatisierten Entscheidungen überwacht bzw. gegebenenfalls Eingriffe ermöglicht, wenn Anomalien oder Fehlfunktionen auftreten. Dazu gehört auch das regelmäßige Durchführen von Stichproben. Ebenso soll nachträglich überprüft und festgestellt werden können, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind.

Dass die betroffenen Personen über die automatisierte Entscheidung entsprechend aufgeklärt werden, ist bereits durch die Transparenzpflichten nach Art. 13 Abs. 2 lit. f und Art. 14 Abs. 2 lit. g DSGVO gewährleistet. Um die Herkunft der Entscheidungen noch leichter erkennbar zu machen, sollen diese entsprechend als automatisierte Entscheidung gekennzeichnet und mit der Amtssignatur des Verantwortlichen (§ 19 E-GovG) versehen werden. Damit wird auch entsprechende Transparenz erreicht.

Im Ergebnis besteht durch die vom Verantwortlichen zu setzenden Maßnahmen, die den Standards des DSG und der DSGVO entsprechen, kein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen (siehe dazu im Allgemeinen Teil unter V. die DSFA).

Zu § 5:

Die DSGVO verpflichtet den Verantwortlichen, über das Bestehen einer automatisierten Entscheidungsfindung aufzuklären sowie aussagekräftige Informationen über die involvierte Logik zur Nachvollziehbarkeit der Entscheidung sowie die Bedeutung und die beabsichtigten Folgen für die betroffene Person darzulegen (vgl. Art. 13 Abs. 2 lit. f, Art. 14 Abs. 2 lit. g, Art. 15 Abs. 1 lit. h DSGVO). Dies dient dazu, eine Überprüfung der durch den Algorithmus vorgenommenen Bewertung und der letztendlich darauf beruhenden Entscheidung zu ermöglichen. Diese Verpflichtungen werden für jene Fälle eingeschränkt, in denen der Datenschutz, schutzwürdige Rechte Dritter oder öffentliche Interessen an der Geheimhaltung einer Offenlegung entgegenstehen.

Bei der Beschaffung bzw. Vergabe öffentlicher Aufträge kann die öffentliche Verwaltung - nach dem Vorbild von Amsterdam - durch die Vorgabe von Bedingungen sowie Informations-/Transparenz-maßnahmen und die Definition zu erfüllender Kriterien „als Nachfrager für ethische und vertrauenswürdige KI agieren und dadurch Märkte definieren, Standards setzen und [ihre] Effizienz steigern. (…) Bei der Beschaffung von KI-Anwendungen für KI-Projekte ist die Innovationsfördernde Öffentliche Beschaffung-Servicestelle (IÖB) ein Ansprechpartner für die Verwaltungsbediensteten. Hier ist neben dem Bundesvergabegesetz auch das White Paper der IÖB-Servicestelle eine erste Orientierung (IÖB 2021). Darüber hinaus sollten bei KI-Anwendungen wichtige ethische Grundsätze, wie sie im „Kriterien- und Maßnahmenkatalog für KI in der Verwaltung (EKIV)“ (siehe Abschnitt 10.1) ausgeführt werden, schon zu Beginn von Entwicklungsprozessen, wie zB vom „Ethics by Design“-Ansatz vorgeschlagen (siehe Abschnitte 10.3 und 11), bedacht werden.“ (AIM AT 2030, 56 und Leitfaden Digitale Verwaltung und Ethik. Praxisleitfaden für KI in der Verwaltung, Version 1.0, 34)

Drei Arten von Informationen könnten dementsprechend bei der Beschaffung moderner Technologien vereinbart werden:

- Technische Transparenz: Informationen über die technische Funktionsweise (zB Einblicke in den zugrundeliegenden Code), denen insbesondere bei einem Audit oder bei erforderlicher „Erklärbarkeit“ (siehe unten) besondere Bedeutung zukommt.
- Verfahrenstransparenz: Der Zweck der Anwendung und die „gesetzten“ Schritte; zB „eine Beschreibung der getroffenen Entscheidungen und Annahmen, welche Art von Daten verwendet wurde, und wie einer möglichen Verzerrung entgegengewirkt wurde. So kann überprüft werden, ob die richtigen Maßnahmen zur Qualitätssicherung und Risikominderung getroffen wurden.”
- Erklärbarkeit: Die Entscheidungsfindung der Anwendung soll auf individueller Ebene transparen sein („Erklärbarkeit“).

Der Zugang zu Quellcodes auch von zugekauften Anwendungen ist maßgeblich, um dem Kriterium der Transparenz gerecht zu werden (siehe dazu auch die Ausführungen zu VI.)

Zu § 6:

Verantwortlicher nach der DSGVO ist, wer allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Die Stelle, die gemäß § 6 dieses Landesgesetzes für die Einhaltung verantwortlich ist, entspricht dem Begriff des Verantwortlichen nach der DSGVO. Diese Stelle muss sicherstellen, dass die von ihr eingesetzte Informationstechnologie die gesetzlichen Vorgaben einhält und die Datenverarbeitung rechtskonform erfolgt. Personen, die durch die Nichteinhaltung des Landesgesetzes in ihren Rechten beeinträchtigt werden, können die bestehenden Rechtsschutzinstrumente (etwa nach der DSGVO bzw. dem DSG) in Anspruch nehmen.

Zu § 7:

Mit dieser Bestimmung werden die den Gemeinden und Gemeindeverbänden zukommenden Aufgaben nach diesem Gesetz entsprechend der Verpflichtung des Art. 118 Abs. 2 B-VG ausdrücklich als Aufgaben des eigenen Wirkungsbereichs bezeichnet.

Zu § 8:

Verweise auf die jeweiligen Fassungen des Artificial Intelligence Acts (AI-Act), der Datenschutz-Grundverordnung (DSGVO), des Datenschutzgesetzes (DSG) und des E-Government-Gesetzes (E-GovG).

Zu § 9:

Diese Bestimmung enthält die In-Kraft-Tretens-Bestimmung.

Landesgesetz

über den Einsatz moderner Informationstechnologien zur Förderung der digitalen Transformation der Verwaltung (Oö. Informationstechnologien-Einsatz-Gesetz)

Der Oö. Landtag hat beschlossen:

INHALTSVERZEICHNIS

§ 1
Ziel und Anwendungsbereich

Ziel dieses Landesgesetzes ist die Förderung eines transparenten und nachvollziehbaren Einsatzes moderner Informationstechnologien durch das Land, die Gemeinden, die Gemeindeverbände und die sonstigen Körperschaften öffentlichen Rechts im Zuständigkeitsbereich des Landes Oberösterreich.

§ 2
Begriffsbestimmungen

Im Sinn dieses Landesgesetzes bedeutet:

1. **automatisiert:** durch Einsatz eines technischen Verfahrens selbstständig ablaufende Datenverarbeitung;
2. **künstliche Intelligenz (KI):** KI-System im Sinn des Art. 3 Z 1 [*Fundstelle/Zitat wird nach Verlautbarung ergänzt werden.*], das assistierende Funktionen ausübt und nicht unter die Kategorie der Hochrisiko-KI-Systeme im Sinn des Art. 6 Abs. 1 und 2 [*Fundstelle/Zitat wird nach Verlautbarung ergänzt werden.*] fällt;
3. **moderne Informationstechnologie:** künstliche Intelligenz und sonstige algorithmisch arbeitende Systeme;
4. **personenbezogene Daten:** personenbezogene Daten im Sinn des Art. 4 Z 7 Datenschutz-Grundverordnung - DSGVO;

5. **sonstige algorithmisch arbeitende Systeme:** Technologien, die auf dem Einsatz von Algorithmen basieren und zur automatisierten Verarbeitung von Daten dienen;
6. **Verantwortlicher:** Verantwortliche oder Verantwortlicher im Sinn des Art. 4 Z 1 DSGVO.

§ 3
Datenverarbeitungen zur Entwicklung moderner Informationstechnologien

(1) Im Anwendungsbereich dieses Landesgesetzes ist die Verarbeitung personenbezogener Daten ausschließlich zum Zweck der Entwicklung moderner Informationstechnologien sowie für das dafür erforderliche Einüben (Trainieren), die erforderliche Überprüfung der Eignung der Methode für einen bestimmten Zweck (Validieren) und das Testen zulässig, wenn dies zur Zweckerreichung erforderlich ist und gleichwertige Ergebnisse nicht ohne unverhältnismäßig hohen Aufwand auf andere Weise mit anonymisierten, anderweitig zusammengefügten (synthetischen) oder sonstigen nicht personenbezogenen Daten wirksam erzielt werden können.

(2) Die personenbezogenen Daten müssen im sachlichen Zusammenhang mit der bestimmungsgemäßen Verwendung der jeweiligen modernen Informationstechnologie stehen, zur Zweckerreichung erforderlich und

1. in ihren Identifikationsmerkmalen soweit ersetzt werden, dass eine Feststellung der Identität der oder des Betroffenen ausgeschlossen ist (pseudonymisiert) oder
2. vom Verantwortlichen für andere Zwecke zulässigerweise ermittelt worden oder
3. über Register von Verantwortlichen des öffentlichen Bereichs zulässiger Weise zugänglich sein.

(3) Bei der Auswahl der Daten nach Abs. 1 ist darauf zu achten, dass diese hinreichend notwendig (relevant), repräsentativ, nicht-diskriminierend, moralisch einwandfrei (integer), objektiv und so weit wie möglich fehlerfrei und im Hinblick auf den verfolgten Zweck vollständig sind.

(4) Die Verarbeitung personenbezogener Daten nach dieser Bestimmung darf zu keinen Maßnahmen oder Entscheidungen führen, die Auswirkungen auf die betroffenen Personen haben.

(5) Der Verantwortliche hat jedenfalls zu dokumentieren:

1. die Herkunft der Daten,
2. im Fall personenbezogener Daten den ursprünglichen Zweck der Datenerfassung, die Datenlieferantin bzw. den Datenlieferanten, den Erhebungszusammenhang (Kontext) und den Erhebungszeitpunkt sowie
3. die Gründe, die Entwicklung sowie die Methoden des Trainierens, Validierens und Testens, den Prozess und die Testergebnisse.

(6) Der Verantwortliche hat unter Beachtung der wirtschaftlichen Vertretbarkeit und des Stands der Technik ausreichende Vorkehrungen für die Gewährleistung der Datensicherheit im Sinn der Art. 24, 25 und 32 DSGVO und des § 6 DSG zu treffen, insbesondere ist sicherzustellen, dass die Daten Unbefugten nicht zugänglich sind und in einer gesicherten Umgebung nach aktuellem technischen Standard verarbeitet werden.

(7) Soweit Verantwortliche gemeinsam personenbezogene Daten im Sinn des Abs. 1 zur Entwicklung moderner Informationstechnologien verarbeiten, sind sie gemeinsam Verantwortliche nach Art. 4 Z 7 in Verbindung mit Art. 26 DSGVO. Die Erfüllung von datenschutzrechtlichen

Informations-, Auskunfts-, Berichtigungs-, Löschungs- und sonstigen Pflichten obliegt jenem Verantwortlichen, der als Anlaufstelle genannt ist.

§ 4
Automatisierte Entscheidungen

(1) Soweit von Verantwortlichen Leistungen als Träger von Privatrechten erbracht werden, ist es zulässig, die dafür notwendigen Entscheidungen durch sonstige algorithmisch arbeitende Systeme im Sinn des § 2 Z 5 vollständig automatisiert vorzunehmen.

(2) Ausfertigungen dieser Entscheidungen haben eine Begründung zu enthalten, müssen als Ergebnis eines automatisierten Entscheidungsprozesses gekennzeichnet sein und sind mit der Amtssignatur (§ 19 E-GovG) des Verantwortlichen zu versehen.

(3) Der Verantwortliche hat zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person angemessene Maßnahmen, die mehrere gleichartige Verarbeitungsvorgänge umfassen können, zu ergreifen. Diese Maßnahmen sind jedenfalls:

1. die Dokumentation, dass die bestimmungsgemäße Funktionsweise des Systems vor Produktivsetzung gründlich überprüft, validiert und getestet wurde,
2. der Einsatz (Implementierung) wirksamer Kontrollen samt regelmäßiger Überprüfung der Richtigkeit und Relevanz der automatisierten Entscheidungen,
3. die Erstellung einer Dokumentation vor Produktivsetzung, die auf dem neuesten Stand zu halten und für einen Zeitraum von zehn Jahren ab Beendigung der Datenverarbeitung aufzubewahren ist und insbesondere Folgendes umfasst:
   a) eine allgemeine Beschreibung inkl. Systemarchitektur und Zweckbestimmung sowie allfällige Interaktion mit anderen Systemen,
   b) aussagekräftige Informationen über die involvierte Logik des algorithmisch arbeitenden Systems,
   c) die ergriffenen technischen und organisatorischen Maßnahmen zur Daten- und Informationssicherheit,
4. die Protokollierung über tatsächlich durchgeführte Verarbeitungsvorgänge (Anwendungsprotokolle), wie beispielsweise Änderungen und Übermittlungen, im zur Nachvollziehbarkeit notwendigen Ausmaß, welche für mindestens sechs Monate gespeichert wird,
5. das Speichern von Logdateien, die aus technischen Gründen geführt werden, für mindestens sechs Monate und
6. geeignete, dem jeweiligen Stand der Technik entsprechende Vorkehrungen für die Verfügbarkeit und Integrität der Daten.

§ 5
Transparenz

Die Pflichten gemäß Art. 13 bis 15 DSGVO bestehen nicht, soweit die ordnungsgemäße Erfüllung der Aufgaben gefährdet würde, insbesondere wenn dadurch Rückschlüsse auf die

Ausgestaltung automationsunterstützter Risikomanagementsysteme möglich wären, die öffentliche Sicherheit oder Ordnung gefährdet würde, überwiegende berechtigte Interessen Dritter geschädigt würden oder der Schutz personenbezogener Daten oder andere öffentliche Interessen an der Geheimhaltung dem entgegenstehen.

§ 6
Verantwortlichkeit

Verantwortlich für die Einhaltung dieses Landesgesetzes ist jene Stelle, die eine moderne Informationstechnologie zur Erledigung der von ihr wahrgenommenen Aufgaben entwickelt, trainiert oder einsetzt.

§ 7
Eigener Wirkungsbereich

Die in diesem Landesgesetz geregelten Aufgaben der Gemeinden, der Gemeindeverbände und sonstiger Selbstverwaltungskörper sind solche des eigenen Wirkungsbereichs.

§ 8
Verweise

(1) Soweit in diesem Landesgesetz auf Unionsrechtsakte verwiesen wird, ist dies als Verweis auf folgende Fassung zu verstehen:

- AI-Act [*Fundstelle/Zitat wird nach Verlautbarung ergänzt werden.*]
- 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), ABl. Nr. L 119 vom 4.5.2016, S 1, in der Fassung der Berichtigung vom 4. März 2021, ABl. Nr. L 74 vom 4.3.2021, S 35.

(2) Soweit in diesem Landesgesetz auf Bundesgesetze verwiesen wird, ist dies als Verweis auf folgende Fassung zu verstehen:

- Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Datenschutzgesetz - DSG), BGBl. I Nr. 165/1999, in der Fassung des Bundesgesetzes BGBl. I Nr. 2/2023;
- Bundesgesetz über Regelungen zur Erleichterung des elektronischen Verkehrs mit öffentlichen Stellen (E-Government-Gesetz - E-GovG), BGBl. I Nr. 10/2004, in der Fassung des Bundesgesetzes BGBl. I Nr. 119/2022.

§ 9
Inkrafttreten

Dieses Landesgesetz tritt mit Ablauf des Tages seiner Kundmachung im Landesgesetzblatt für Oberösterreich in Kraft.