



LANDKREIS LÜNEBURG



intellex

Richtlinie zur Nutzung der
KI-Anwendung intellex

Wichtige Informationen zum Dokument	
Dokumenttitel:	Richtlinie zur Nutzung der KI-Anwendung intellex
Verantwortliche/r Autor/in:	Julia Eichler
Versionsnummer:	0.6
Letzte Bearbeitung am:	01.06.2026
Vertraulichkeitsstufe:	Intern
Bearbeitungsstatus:	Freigabe
Freigabe am:	Siehe Verfügungsworkflow
Freigegeben durch:	LR

Änderungshistorie				
Versionsnummer	Status	Datum letzte	Bearbeiter/in	Änderung/ Bemerkung
0.1	Entwurf	05.05.2026	J. Eichler	Ersterstellung
0.2	Entwurf	13.05.2026	J. Eichler	Abstimmung FDL 03
0.3	Entwurf	15.05.2026	J. Eichler	Abstimmung FBL 3
0.4	Entwurf	18.05.2026	J. Eichler	Abstimmung DSB, ITSB
0.5	Entwurf	28.05.2026	J. Eichler	Vorlage Personalrat
0.6	Freigabe	01.06.2026	J. Eichler	Zur Freigabe an FDL 03, FB 3, LR

1. Zweck

Diese Richtlinie regelt die zulässige und datenschutzkonforme Nutzung der KI-Anwendung intellex durch die Mitarbeitenden des Landkreises Lüneburg. Sie dient der Sicherstellung der Vertraulichkeit und Rechtmäßigkeit gemäß den Vorgaben des EU AI Acts, der Datenschutzgrundverordnung (DSGVO) und des Bundes- und Landesdatenschutzgesetzes (BDSG und NDSG).

2. Geltungsbereich

Diese Richtlinie gilt für alle Mitarbeitenden der Kreisverwaltung Lüneburg, die die KI-Anwendung intellex benutzen.

3. Verantwortlichkeit

Der oder die jeweilige Mitarbeitende, der/die KI-Anwendung intellex nutzt, ist verantwortlich für die ordnungsgemäße Durchführung der Dateneingabe und -verarbeitung sowie die Einhaltung dieser Richtlinie.

4. Regeln für die Nutzung von intellex

- Vor der Nutzung von intellex muss eine Schulung zur Anwendung besucht werden. Außerdem muss die Dienstanweisung zur Nutzung von KI nachweisbar zur Kenntnis genommen werden sowie eine allgemeine Schulung zum Thema KI besucht worden sein.
- Die KI-Anwendung intellex darf ausschließlich für dienstliche Zwecke und im Rahmen der zugewiesenen Aufgaben genutzt werden. Jegliche private Nutzung oder der Missbrauch der Anwendung ist untersagt.
- Es dürfen ausschließlich Daten in intellex eingegeben und verarbeitet werden, die gemäß der Klassifizierung der Schutzstufe D oder niedriger zugeordnet sind sowie dem Schutzbedarf hoch der Informationssicherheit. Die Eingabe von Daten der Schutzstufen E (streng vertraulich) sowie dem Schutzbedarf sehr hoch der Informationssicherheit ist strikt untersagt. Siehe hierzu Anhang „Schutz der Vertraulichkeit“
Daten der Schutzstufe E umfassen z.B. Adressen von verdeckten Ermittlern, Daten und Aufenthaltsorte von gefährdeten Personen (z.B. potenzielle Opfer von Straftaten, Zeugenschutz).
- Mitarbeitende sind verpflichtet, vor der Eingabe von Daten deren Schutzstufe zu prüfen und sicherzustellen, dass diese den Vorgaben entsprechen.
- Nach Abschluss der Verarbeitung sind alle eingegebenen, sensiblen Daten der Schutzstufe D unverzüglich (d.h. ohne schuldhaftes Zögern) und unwiederbringlich (d.h. so, dass die Daten nicht wiederhergestellt werden können) aus intellex zu löschen. Eine automatische Löschung der Daten erfolgt nach 90 Tagen.
- Es dürfen nur die für den jeweiligen Verarbeitungsprozess in intellex unbedingt erforderlichen Daten eingegeben werden (Grundsatz der Datenminimierung).
- Die Nutzung der in intellex verarbeiteten Daten ist ausschließlich für den vorgesehenen Zweck zulässig. Dies bedeutet, dass Sie nur die Daten in intellex eingeben dürfen, die für den jeweiligen Verarbeitungsprozess unbedingt erforderlich sind und für die Bearbeitung Ihrer Aufgabe benötigt werden.
- Es ist sicherzustellen, dass der Einsatz von intellex nicht zu Diskriminierungen insbesondere aufgrund von Geschlecht, ethnischer Herkunft, Religion, Weltanschauung, Behinderung, Alter oder sexueller Identität führt.
- Die Mitarbeitenden sind verpflichtet, die von der KI-Anwendung intellex generierten Ergebnisse kritisch zu prüfen und zu validieren, bevor diese für Entscheidungen oder weitere Verarbeitungsschritte herangezogen werden. Die KI dient als unterstützendes Werkzeug, die Letztverantwortung für die Ergebnisse und daraus resultierende Handlungen verbleibt stets beim Menschen.

Besonders zu beachten sind neben den genannten Punkten die Leitlinie zur Informationssicherheit und den Datenschutz. Diese ist in den Hausinformationen zu finden.

5. Schlussbestimmungen

Konsequenzen bei Nichteinhaltung: Verstöße gegen diese Richtlinie können disziplinarische oder arbeitsrechtliche Maßnahmen nach sich ziehen und im Falle von Datenschutzverstößen rechtliche Konsequenzen haben.

6. Inkrafttreten

Diese Richtlinie tritt am 01.06.2026 in Kraft. Änderungen oder Ergänzungen dieser Richtlinie müssen vom Landrat genehmigt werden.

Schutz der Vertraulichkeit						
DS-GVO				Informationssicherheit		
Recht auf Schutz personenbezogener Daten				Schutzbedarf feststellung aller Informationen		
Schutzstufe	Personenbezogene Daten	Beispiel	Schwere eines möglichen Schadens	Schutzbedarf	Auswirkungen	
A	die von den Betroffenen freizugänglich gemacht wurden.	Telefonverzeichnis, Wahlvorschlagsverzeichnisse, eigene freizugänglichgemachte Webseite; frei zugängliche soziale Medien	geringfügig	normal	Die Schadenauswirkungen sind begrenzt und überschaubar	• Verstoß gegen Gesetze/Vorschriften/Verträge, • Beeinträchtigung des informationellen Selbstbestimmungsrechts, • Beeinträchtigung der persönlichen Unversehrtheit • Beeinträchtigung der Aufgabenerfüllung, • negative Innen- oder Außenwirkung und • finanzielle Auswirkungen.
B	deren unsachgemäße Handhabung zwar keine besondere Beeinträchtigung erwarten lässt, die aber von den Betroffenen nicht frei zugänglich gemacht wurden.	beschränkt zugängliche öffentliche Dateien, Verteiler für Unterlagen, Grundbucheinsicht; nicht frei zugängliche soziale Medien				
C	deren unsachgemäße Handhabung den Betroffenen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigen könnte („Ansehen“).	Einkommen, Grundsteuer, Ordnungswidrigkeiten	überschaubar			
D	deren unsachgemäße Handhabung den Betroffenen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen erheblich beeinträchtigen könnte („Existenz“).	Anstaltsunterbringung, Straffälligkeit, dienstliche Beurteilungen, Arbeitszeugnisse, Gesundheitsdaten, Schulden, Pfändungen, Sozialdaten, Daten besonderer Kategorien nach Art. 9 DS-GVO	substantiell	hoch	Die Schadenauswirkungen können beträchtlich sein.	
E	deren unsachgemäße Handhabung Gesundheit, Leben oder Freiheit des Betroffenen beeinträchtigen könnte.	Daten über Personen, die mögliche Opfer einer strafbaren Handlung sein können, Zeugenschutzprogramm.	groß	sehr hoch	Die Schaden- auswirkungen können ein existenziell bedrohliches, katastrophales Ausmaß erreichen	