

Dienstvereinbarung zur Einführung und Anwendung von ALLRIS zwischen der Carl von Ossietzky Universität Oldenburg (Dienststelle) und dem Personalrat der Carl von Ossietzky Universität Oldenburg

vom 11.05.2020

§ 1 Ziele und Grundsätze

- (1) Diese Dienstvereinbarung soll einerseits die Verarbeitung personenbezogener Daten der Beschäftigten beim Einsatz der Software ALLRIS transparent machen und andererseits die Verarbeitung personenbezogener Daten festlegen.
- (2) Ziel ist, den Schutz der Persönlichkeitsrechte der Beschäftigten (Datenschutz) zu gewährleisten.

§ 2 Gegenstand und Geltungsbereich

- (1) Diese Dienstvereinbarung regelt die Einführung und Anwendung der Software ALLRIS in der Universität einschließlich der dafür eingesetzten Hardware und vor- und nachgelagerter Systeme (nicht abschließend: Webserver, Datenbankserver, Backupsysteme, Übertragungseinrichtungen wie Proxies und Firewalls). Sie gilt für alle Beschäftigten der Universität Oldenburg.
- (2) Soweit personelle oder andere Maßnahmen mit der Einführung und Anwendung der Software ALLRIS im Zusammenhang stehen oder aus ihr folgen, finden die entsprechenden gesetzlichen Bestimmungen Anwendung, soweit diese Dienstvereinbarung keine abweichenden Regelungen trifft.

§ 3 Einsatzzweck

Der Einsatz der Software ALLRIS dient ausschließlich folgenden Zwecken:

- Digitale Erstellung, Einreichung, Bearbeitung und Zugänglichmachung von Anträgen und Sitzungsunterlagen, ihre Nutzung in den Sitzungen der universitären Gremien durch die Gremienmitglieder sowie die digitale Erzeugung der zugehörigen Gremienbeschlüsse und -protokolle sowie ihre Veröffentlichung.
- Unterstützung der Prozesse der universitären Gremien sowie anderer Organisationseinheiten, die in die digitale Sitzungsvor- und -nachbereitung eingebunden sind bzw. im Falle einer Antrags- oder Vorlagenerstellung.

Die universitären Gremien, in denen ALLRIS eingesetzt wird, können der Anlage unter I. „Einsatzbereiche“ entnommen werden.

Die Verarbeitung personenbezogener Daten findet ausschließlich in dem in dieser Dienstvereinbarung festgelegten Rahmen statt.

§ 4 Verarbeitung personenbezogener Daten (Allgemeiner Teil)

- (1) Die in ALLRIS verwalteten personenbezogenen Daten sowie die zugriffsberechtigten Personen auf die Software ALLRIS für die einzelnen Gremien sind der Anlage unter II. „Verarbeitung personenbezogener Daten (Besonderer Teil)“ zu entnehmen. Mitarbeiter*innen (auch u. a. Leitungen, Gremienvorsitz, Vertretung) aus anderen Organisationseinheiten haben einen Zugang u.- a. für die Vorlagenerstellung und die Verarbeitung von Beschlüssen. Sofern es für ihre jeweilige Aufgabenerfüllung notwendig ist, können weitere Personen aus Organisationseinheiten der Universität einen lesenden Informationszu-

gang zu den Unterlagen einzelner Gremien erhalten. Sie kommen ausnahmslos aus dem Kreis der Beschäftigten, die abschließend in § 4 Abs.1 NPersVG genannt sind. Gremienmitglieder (auch externe Personen) haben einen lesenden Zugriff auf ALLRIS.

(2) Schnittstellen zu anderen Datenquellen:

Aus dem Identity-Management-System der Universität werden über eine LDAP-Schnittstelle die zum Login benötigten Personendaten und die Merkmale Name, Organisationseinheit dienstliche Telefonnummer, E-Mail-Adresse, Benutzerkennung, Statusgruppe, Rolle im Gremium in das System übertragen.

(3) Protokollierungen:

In ALLRIS wird protokolliert, von wem wann der Status einer Vorlage, eines Beschlusses, einer Tagesordnung und eines Protokolls verändert wird. Diese Merkmale werden solange gespeichert, wie diese Dokumente in ALLRIS vorhanden sind.

Im ALLRIS Ereignisprotokoll werden die Aktivitäten der Nutzer*innen protokolliert. Die Ereigniseinträge werden unstrukturiert fortlaufend in die Datei geschrieben. Die Ereigniseinträge werden in genau eine Ereignisdatei geschrieben. Ereignisse sind z. B. die Anmeldung eines Nutzers, das Aufrufen von Microsoft OFFICE für die Vorlagenbearbeitung, der Versand einer E-Mail aus ALLRIS mit Betreff und Empfänger*in.

Die von ALLRIS angebotene Funktion „Beschlussverfolgung“ und sowie einige andere Funktionen (z. B. „Sitzungsgeld“) werden nicht genutzt.

Außerhalb von ALLRIS protokolliert der Webserver, wann von welcher Client-IP-Adresse welche Resource aufgerufen wurde.

§ 5

Schutz der Beschäftigten vor unzulässiger Überwachung

Das System ALLRIS inklusive seiner vor- und nachgelagerten Systeme (nicht abschließend: Webserver, Datenbankserver, Backupsysteme, Übertragungseinrichtungen wie Proxies und Firewalls) und die im Rahmen des Betriebs oder der Einführung erhobenen, gespeicherten und/oder verarbeiteten Daten dürfen nicht zur Leistungs- und/oder Verhaltenskontrolle der Arbeitnehmer*innen genutzt werden. Dies gilt auch für die Kontrolle der Leistung und/oder des Verhaltens einer Gruppe von Beschäftigten.

§ 6

Maßnahmen zur Sicherung der Daten, Lösungsfristen, Grundsatz der Datensparsamkeit

(1) Die Daten werden auf Systemen der Universität Oldenburg (IT-Dienste) gespeichert, die in nicht allgemein zugänglichen Räumen aufgestellt sind. Zu diesen Systemen haben lediglich Administrator*innen eine Zugriffsberechtigung. ~~Mitarbeiter*innen (auch u. a. Leitungen, Gremienvorsitz, Vertretung) aus anderen Organisationseinheiten haben einen Zugang u. a. für die Vorlagenerstellung und die Verarbeitung von Beschlüssen. Sofern es für ihre jeweilige Aufgabenerfüllung notwendig ist, können weitere Personen aus Organisationseinheiten der Universität einen lesenden Informationszugang zu den Unterlagen einzelner Gremien erhalten. Sie kommen ausnahmslos aus dem Kreis der Beschäftigten, die abschließend in § 4 Abs.1 NPersVG genannt sind. Gremienmitglieder (auch externe Personen) haben einen lesenden Zugriff auf ALLRIS.~~

(2) Für den Betrieb von ALLRIS und alle vor- und nachgelagerten Systeme gilt in Bezug auf personenbezogene oder -beziehbare Daten der Grundsatz der Datensparsamkeit. Eine statistische Auswertung der Nutzung von ALLRIS – auch auf Grundlage aggregierter Daten – findet nicht statt.

(3) Die technische Administration erfolgt durch die IT-Dienste der Universität Oldenburg.

(4) Für die inhaltliche Administration sind die Mitarbeiter*innen der den Organisationseinheiten zugeordneten Gremien der Carl von Ossietzky Universität Oldenburg verantwortlich. Die einzelnen Organisationseinheiten können der Anlage unter II. „Zugriffsberechtigte Personen“ entnommen werden.

(5) Die maximale Speicherfrist für die im Ereignisprotokoll von ALLRIS sowie in den Logdateien des Webserver und aller anderen vor- und nachgelagerten Systeme gespeicherten Daten beträgt eine Woche. Die Löschung erfolgt automatisiert.

(6) Besteht die begründete Vermutung eines Missbrauchs des Systems oder eines technischen Fehlers, kann die Speicherfrist für Daten nach Abs. 5 auf maximal drei Monate verlängert werden. Die verlängerte Speicherfrist gilt nur für die Daten, die seit Auftreten der Vermutung des Missbrauchs oder technischen Fehlers bis zur Klärung des Sachverhalts anfallen, oder so lange die Daten zur Erfolgskontrolle von Maßnahmen zur Störungsbeseitigung benötigt werden. Der Datenschutzbeauftragte ist einzubeziehen.

Der Personalrat wird unverzüglich jeweils über Beginn und Ende der verlängerten Speicherfrist, über den auslösenden Sachverhalt, über die Analyseergebnisse, die endgültige Löschung der Daten und die ggf. veranlassten Maßnahmen informiert.

(7) Soweit Daten nach Absatz 5 zur Durchsetzung zivilrechtlicher Ansprüche gegen den Hersteller von ALLRIS oder andere externe Dienstleister und Lieferanten der Universität als Beweismittel benötigt werden, sind sie abweichend von Absatz 6 spätestens nach Abschluss des gerichtlichen Verfahrens zu löschen. Dies gilt analog bei Erstattung einer Strafanzeige bis zum Abschluss des gerichtlichen Verfahrens oder bis zur Einstellung des Ermittlungsverfahrens.

(8) Soweit vertrauliche Unterlagen, die über ALLRIS bereitgestellt wurden, den Kreis der berechtigten Adressaten verlassen, und diese Unterlagen mit einem auf eine*n einzelne*n berechnete*n Nutzer*in bezieharen Wasserzeichen oder Abrufvermerk versehen sind, ist dennoch die Unschuld der*des Nutzer*in zu vermuten. Die Beweislast für einen vermuteten Verstoß gegen die Verpflichtung zur Verschwiegenheit obliegt der Dienststelle. Hochschulöffentliche Unterlagen werden nicht mit einem Wasserzeichen oder Abrufvermerk versehen.

§ 7

Rechte des Personalrats

(1) Änderungen und Erweiterungen des Systems ALLRIS und seiner Einsatzzwecke bedürfen einer Änderung dieser Dienstvereinbarung.

(2) Der Personalrat hat gegenüber der Dienststelle ein umfassendes Informationsrecht zur Überprüfung der Einhaltung dieser Dienstvereinbarung. Insbesondere sind Maßnahmen nach § 6 Absätze 6 - 8 auf Verlangen mit dem Personalrat zu erörtern.

§ 8

Beschwerderecht

Soweit sich Beschäftigte bei der Dienststelle über die Folgen der getroffenen Maßnahmen und Regelungen oder über die Nichteinhaltung beschweren, ist der Personalrat zu informieren, es sei denn, dass dies von der*dem Beschäftigten ausdrücklich nicht gewollt ist. Dienststelle und Personalrat bemühen sich gemeinsam, berechtigten Beschwerden abzuwehren. Das Recht der*des einzelnen Beschäftigten, sich direkt an den Personalrat zu wenden, bleibt davon unberührt.

§ 9

Schlussbestimmungen

(1) Die Dienstvereinbarung tritt mit der Veröffentlichung in den Amtlichen Mitteilungen in Kraft. Sie ersetzt die Dienstvereinbarung vom 20.12.2017, zuletzt geändert am 12.12.2019.

(2) Die Dienstvereinbarung kann mit einer Frist von vier Monaten von beiden Seiten gekündigt werden. Die einvernehmliche Änderung ist jederzeit möglich. Kündigung und Änderung bedürfen der Schriftform.

(3) Diese Dienstvereinbarung gilt auch für Gremien, die sich im vom Personalrat genehmigten Testbetrieb mit ALLRS befinden. Im Testbetrieb befindliche Gremien sind der Anlage unter III. „Testbetrieb“ zu entnehmen. Die im Zusammenhang mit der Beantragung des Betriebs beim Personalrat eingereichten Unterlagen und Verfahrensbeschreibungen sind Anlagen dieser Dienstvereinbarung.

(4) Die Anlage ist Bestandteil der Dienstvereinbarung. Sie kann nur im Einvernehmen zwischen Dienststelle und Personalrat geändert werden.

gez. Prof. Dr. Dr. Hans Michael Piper
(Präsident)

gez. Petra Mende
(Vorsitzende des Personalrats)

Anlage zur Dienstvereinbarung

I. Einsatzbereiche

- **Gremium:** Präsidium
 - o **Organisationseinheit:** Geschäftsbereich Präsidiumsbetreuung des Referats Präsidiums- und Gremienbetreuung, Allgemeine Rechtsangelegenheiten (PGR)
- **Gremien:** Senat, Senatskommissionen und Promovierendenvertretung
 - o **Organisationseinheit:** Zentrales Gremienbüro des Referats Präsidiums- und Gremienbetreuung, Allgemeine Rechtsangelegenheiten (PGR)
- **Gremien:** Studienqualitätskommission und Fakultätsübergreifende Studienkommission
 - o **Organisationseinheit:** Referat Studium und Lehre, Sachbearbeitung Studienqualitätskommission und Fakultätsübergreifende Studienkommission
- **Gremium:** Fakultätsrat der Fakultät III
 - o **Organisationseinheit:** Geschäftsstelle des Dekanats der Fakultät III

II. Verarbeitung personenbezogener Daten (Besonderer Teil)

(1) Verwaltet werden folgende personenbezogenen Daten:

Sitzungen des Präsidiums

Name, Organisationseinheit, dienstliche Telefonnummer, E-Mail-Adresse, Benutzerkennung, Funktionsbezeichnung von Sitzungsteilnehmer*innen, Berichterstatter*innen und anderen Beteiligten (z. B. externe Personen) sowie der Beschäftigten im Referat PGR/Geschäftsbereich Präsidiumsbetreuung.

Sitzungen des Senats, der Senatskommissionen und der Promovierendenvertretung

Name, Organisationseinheit, dienstliche Telefonnummer, E-Mail-Adresse, Benutzerkennung, Funktionsbezeichnung von Sitzungsteilnehmer*innen, Berichterstatter*innen und anderen Beteiligten (z. B. externe Personen) sowie der Beschäftigten im Referat PGR/Zentrales Gremienbüro.

Sitzungen der Studienqualitätskommission und der Fakultätsübergreifenden Studienkommission

Name, Organisationseinheit, dienstliche Telefonnummer, E-Mail-Adresse, Benutzerkennung, Funktionsbezeichnung von Sitzungsteilnehmer*innen, Berichterstatter*innen und anderen Beteiligten (z. B. externe Personen) sowie der Beschäftigten im Referat Studium und Lehre.

Sitzungen des Fakultätsrats der Fakultät III

Name, Organisationseinheit, dienstliche Telefonnummer, E-Mail-Adresse, Benutzerkennung, Funktionsbezeichnung von Sitzungsteilnehmer*innen, Berichterstatter*innen und anderen Beteiligten (z. B. externe Personen) sowie der Beschäftigten in der Fakultät III/Geschäftsstelle des Dekanats.

(2) Zugriffsberechtigte Personen:

Verwaltung und Gremienmitglieder

Einen umfassenden Zugriff auf die Software ALLRIS haben die Support-Mitarbeiter*innen der IT-Dienste der Abteilung IT-AS und die ALLRIS-Administration.

Die Mitarbeiter*innen (auch u. a. Leitungen, Gremienvorsitz, Vertretung) der folgenden Organisationseinheiten haben Zugriff auf die Sitzungsvorbereitung, -durchführung und -nachbereitung sowie Gremienadministration der ihrer jeweiligen Organisationseinheit zugeordneten Gremien:

- Zentrales Gremienbüro des Referats PGR
- Geschäftsbereich Präsidiumsbetreuung des Referats PGR
- Geschäftsstelle des Referats Studium und Lehre der FÜSK und der SQK
- Geschäftsstelle des Dekanats der Fakultät III

Support

Zugriff auf die virtuellen Server (Test- und Produktionssystem) haben die Support-Mitarbeiter*innen der IT-Dienste, Abteilung Desktop Services. Dem Hersteller CC e-gov wird bei Bedarf zeitlich begrenzt ein VPN-Tunnel zu den virtuellen Servern (z. B. für Updates) bereitgestellt. Ferner kann der Hersteller CC e-gov zu Supportzwecken per „fastviewer“ hinzugeschaltet werden. Der Zugriff von CC e-gov wird durch die „Vereinbarung zur Datenverarbeitung im Auftrag“ geregelt.

III. Testbetrieb

Folgende Gremien befinden sich zurzeit im Testbetrieb:

Gremium	Zeitraum des Testbetriebs
Studienqualitätskommission	bis zum 31.12.2020
Fakultätsübergreifende Studienkommission	bis zum 31.12.2020