

Dienstvereinbarung zur Regelung des Betriebs des Landeskirchenweiten Intranets (LKI) in der Evangelischen Kirche Berlin-Brandenburg- schlesische Oberlausitz (EKBO)

Vom 11./18. November 2024

Zwischen

der Kirchenleitung der Evangelischen Kirche Berlin-Brandenburg-schlesische Oberlausitz, vertreten durch die Präsidentin des Konsistoriums (nachfolgend DL),

und

der Hauptmitarbeitervertretung (nachfolgend HMAV), vertreten durch den Vorsitzenden, wird folgende Dienstvereinbarung geschlossen:

Inhalt

Präambel

1. Geltungsbereich und Verantwortlichkeiten
2. Ziele und Zwecke
3. Beteiligung der Mitarbeitervertretungen
4. Koordinierungsausschuss
5. Schulungen, Informationsmaterial
6. Recht auf Nichterreichbarkeit
7. Benutzerservice
8. Private Nutzung
9. Datenschutz und Datensicherheit
10. Abwesenheit, Vertretung und Ausscheiden von Mitarbeiter:innen
11. Seelsorge
12. Schlussbestimmungen

Übersicht der Anlagen

- Anlage 1 – Schulungskonzept
- Anlage 2 – Katalog der Beschäftigendaten
- Anlage 3 – Datenschutzfolgeabschätzung (mit drei Unteranlagen) – vom Abdruck wurde abgesehen
- Anlage 4 – Stellungnahme des örtlich Beauftragten für den Datenschutz vom 7. März 2024 – vom Abdruck wurde abgesehen
- Anlage 5 – Rechte- und Rollenkonzept

Präambel

Die Parteien der vorliegenden Dienstvereinbarung wollen mit der Einführung eines Landeskirchenweiten Intranets (LKI) neue, einfachere und schnellere, zugleich ressourcenschonende, Informations- und Kommunikationsmöglichkeiten schaffen. Den Unterzeichnenden ist bewusst, dass insbesondere die Sicherheit der personenbezogenen Daten gewährleistet werden muss. Der Zugang und die Nutzung des LKI soll barrierefrei möglich sein.

1. Geltungsbereich und Verantwortlichkeiten

- 1.1. Diese Regelung gilt für alle Mitarbeiterinnen und Mitarbeiter i. S. v. § 2 Absatz 1 MVG-EKD i. V. m. § 2 MVG-AG der Körperschaften, Einrichtungen und rechtlich unselbständigen Werke der EKBO, die das Landeskirchenweite Intranet der EKBO (nachfolgend LKI) nutzen. Sie ist in gleicher Weise für die Dienststellenleitungen verbindlich.
- 1.2. Die Landeskirche, vertreten durch die Präsidentin oder den Präsidenten des Konsistoriums, betreibt das LKI für die Körperschaften der EKBO. Sie ist die verantwortliche Stelle im Sinne des Datenschutzgesetzes der EKD für das von ihr betriebene LKI.
- 1.3. Verantwortliche und Ansprechpartner:
 - 1.3.1 Verantwortlich für Unterstützung und Support bei Anfragen der Nutzerinnen und Nutzer: CANCOM-UHD (User Help Desk) im Auftrag der EKBO.
 - 1.3.2 Verantwortlich für Dienstleistersteuerung und Koordination und Ansprechpartner für die HMAV ist die LKI-Leitung (derzeit Sachgebietsleitung 1.3.2). Die Leitung des LKI steht den Mitarbeitervertretungen als Ansprechpartner in Fragen der Gestaltung des Verfahrens und der Beteiligung zur Verfügung. Sie trägt Verantwortung für die Umsetzung dieser Dienstvereinbarung. In ihrer Funktion nehmen sie

insbesondere folgende Aufgaben im Rahmen der prozessbegleitenden Beteiligung wahr:

- a) Bereitstellung und Übermittlung von Informationen über das Verfahren gemäß 3.1.,
 - b) Beteiligung der Mitarbeitervertretungen im Zuge von Änderungen des Verfahrens gemäß 3.1. und 3.2.
- 1.3.3 1 Verantwortlich für die Identifikation von Nutzer:innen sowie die Rechtevergabe sind die Vertrauensinstanzen in den Kirchenkreisen. 2 Jeder Kirchenkreis benennt mindestens eine Person als Vertrauensinstanz und eine weitere als Stellvertretung.
- 1.3.4 Verantwortlich für die Begleitung der jeweils Zuständigen in Fragen der IT-Sicherheit ist die oder der Beauftragte für IT-Sicherheit im Konsistorium.
- 1.3.5 Verantwortlich für die Begleitung der jeweils Zuständigen in Fragen des Datenschutzes ist die oder der örtliche Beauftragte für den Datenschutz im Konsistorium.
- 1.3.6 1 Die Mitglieder des Koordinierungsausschusses sind verantwortlich für die Vorbereitung der Entscheidung von Grundsatzfragen sowie Unterstützung der Beteiligungsprozesse gegenüber den Gremien HMAV und Pfarrvertretung bei Änderungen, insbesondere der Einführung neuer Module für das LKI. 2 Die Ansprechpartnerinnen und Ansprechpartner gemäß 1.3.2 sind an geeigneter Stelle bekannt zu machen.

2. Ziele und Zwecke

- 2.1. 1 Das LKI wird insbesondere zur Kommunikation der Nutzer:innen untereinander, für die Selbstverwaltung von Terminen (Kalenderfunktion) zur gemeinsamen Bearbeitung und Speicherung von Dokumenten in einer Nutzergruppe zur Verfügung gestellt.

2 Zu diesen Zwecken werden folgende Module im LKI eingesetzt:

- E-Mail, Kalender, Kontakte,
- Dokumentenablage und Verwaltung (Safe),
- EKBO Dialog (Chat/Messenger),
- EKBOfairMeet (Video),
- Terminumfrage,
- Fundus (Bilddatenbank),
- Hilfeforum,
- TYPO3 (Backend-Anmeldung über LKI, künftig),
- EKBO-Termine,
- Coronic Computercheck (künftig, derzeit deaktiviert),

- Bandbreitencheck (künftig),
- Etherpad,
- Intranet des Konsistoriums (künftig),
- Digitale Bibliothek (im Aufbau).

3Die Einbindung weiterer Module oder Ersatz von Modulen durch andere technische Lösungen unterliegt der Mitbestimmung nach dem MVG.EKD, sofern Mitbestimmungstatbestände berührt sind. 4Die Beteiligten klären jeweils, ob eine Änderung dieser Dienstvereinbarung oder eine eigene Dienstvereinbarung erforderlich ist.

2.2. Besondere Ziele dieser Dienstvereinbarung sind:

- eine bestmögliche Gestaltung der IT-gestützten Arbeitsplätze und der Schutz der Beschäftigten vor Gesundheitsschädigungen und Arbeitsüberlastungen,
- der Ausschluss unzulässiger individueller Verhaltens- und Leistungskontrollen und der Schutz personenbezogener Daten der Beschäftigten,
- die Qualitätssicherung der Aus- und Fortbildung aller Beschäftigten im Hinblick auf das LKI.

2.3. Die Parteien sind sich einig, dass das LKI auch anderen in der Kirche Beschäftigten, insbesondere Ehrenamtlichen und Pfarrerinnen und Pfarrern, zur Verfügung steht, auch wenn dies kein Regelungsgegenstand dieser Dienstvereinbarung sein kann.

3. **Beteiligung der Mitarbeitervertretungen**

3.1. 1Alle künftigen wesentlichen Änderungen des LKI-Verfahrens, wie insbesondere die Nutzung neuer Module, Dienstprogramme, Funktionen und Schnittstellen sowie Änderungen der Erhebung und Verarbeitung von Beschäftigtendaten, sind der HMAV und für den Fall, dass diese Änderungen nur einzelne Dienststellen betreffen, den örtlichen Mitarbeitervertretungen nach Maßgabe des Mitarbeitervertretungsrechts rechtzeitig, umfassend und in angemessener Form mitzuteilen. 2Die Informationen müssen so erfolgen, dass die HMAV bzw. die zuständigen Mitarbeitervertretungen ihre Mitwirkungs- und Mitbestimmungsrechte effektiv wahrnehmen können. 3Die Informationen müssen die möglichen Folgen und Auswirkungen der Änderungen ersichtlich und beurteilbar machen.

3.2. Änderungen des LKI-Verfahrens bedürfen der Zustimmung der HMAV und erfordern eine entsprechende Dokumentation und Änderung der entsprechenden Dienstvereinbarung bzw. ihrer Anlagen.

3.3. 1Die Vertragswerke mit den IT-Dienstleistern, die wesentliche Komponenten des LKI zur Verfügung stellen, werden für die HMAV im Intranet in der jeweils geltenden Fassung hinterlegt. 2Alle Beteiligten beachten die vertraglichen und gesetzlichen Verschwiegenheitspflichten.

4. **Koordinierungsausschuss**

1Der Koordinierungsausschuss dient dem Ausgleich der Interessen der verschiedenen Beschäftigtengruppen und Dienststellen und der vertrauensvollen Abstimmung der Weiterentwicklung des LKI im Sinne des größtmöglichen Nutzens für alle Beteiligten. 2Der Ausschuss dient zugleich der Information der HMAV, damit diese ihre Rechte wahrnehmen kann. 3Zum Koordinierungsausschuss gehören:

- zwei Mitglieder, die von der HMAV benannt werden,
- zwei Mitglieder, die von der Pfarrvertretung benannt werden,
- zwei Mitglieder, die von Konsistorium oder Kirchenleitung beauftragt werden,
- der/die örtlich Beauftragte für den Datenschutz.

4Der Koordinierungsausschuss gibt sich eine Geschäftsordnung.

5. **Schulungen, Informationsmaterial**

5.1. 1Die Dienststellenleitung vor Ort soll eine bedarfsgerechte Qualifizierung aller Beschäftigten gewährleisten, die mit dem LKI arbeiten. 2Die Landeskirche bietet Schulungen an. 3Die entsprechende Anlage 1 – Schulungskonzept wird dieser Vereinbarung beigelegt.

5.2. Die Schulungen werden so konzipiert, dass sie:

- ein Verständnis des Aufbaus und der Dialogführung des LKI vermitteln, das die Beschäftigten in die Lage versetzt, das System sicher und effizient zur Erfüllung ihrer Aufgaben zu bedienen,
- Kenntnisse über nutzerfreundliche Einstellungs- und Bedienmöglichkeiten im LKI vermitteln,
- Kenntnisse über einschlägige sicherheitstechnische und datenschutzrechtliche Aspekte (Probleme, Rechtsvorschriften, Maßnahmen und Verhaltensrichtlinien) der Arbeit mit dem LKI vermitteln.

5.3. 1Die Landeskirche trägt die Kosten der Anwenderschulungen mit Ausnahme der Reisekosten. 2Die Reisekosten der Nutzerinnen und Nutzer trägt die entsendende Dienststelle.

5.4. Dienststellenleitungen und Mitarbeitenden wird ausreichend Informationsmaterial zur Verfügung gestellt, um mit dem LKI effektiv arbeiten zu können.

6. **Recht auf Nichterreichbarkeit**

1Dienstliche Kommunikation außerhalb der betriebsüblichen Arbeitszeiten ist nicht erwünscht, soweit keine abweichende arbeitsvertragliche Vereinbarung besteht. 2Eine Pflicht zur ständigen Erreichbarkeit besteht nicht. 3Anfragen über das Landeskirchenweite Intranet müssen daher auch nicht außerhalb der Arbeitszeit bearbeitet werden.

7. **Benutzerservice**

- 7.1. ¹Zur Unterstützung der Nutzer:innen bei der Bedienung des Systems und im Umgang mit Fehlern und sonstigen Problemen der Anwendung des LKI sowie zur nachhaltigen Gewährleistung und Optimierung der Gebrauchstauglichkeit des Systems wird eine Verfahrensbetreuung mit einem Benutzerservice (First Level Support) und einem Änderungsmanagement eingerichtet. ²Das Konsistorium beauftragt einen Dienstleister mit dem First Level Support. ³Der Leistungsschein in seiner jeweiligen Fassung (Bestandteil des Vertrages) wird für die HMAV und Pfarrvertretung im Cloudspeicher hinterlegt, vgl. Nr. 3.3.).
- 7.2. ¹Die Vertragsparteien sind sich einig, dass zur Umsetzung der Ziele dieser Vereinbarung und für die Gewährleistung einer effizienten, datenschutz- und gesundheitsgerechten sowie gute Arbeitsbedingungen fördernden Nutzung des LKI ausreichende personelle Ressourcen im zuständigen Referat erforderlich sind. ²Diese Mitarbeitenden müssen über die notwendigen Qualifikationen zur Dienstleistersteuerung sowie zur Gewährleistung eines nachhaltigen, anwenderbezogenen Systems verfügen.

8. **Private Nutzung**

- 8.1. ¹Das LKI ist aus datenschutz- und telekommunikationsrechtlichen Gründen grundsätzlich nur für den Dienstgebrauch bestimmt. ²Zum Dienstgebrauch gehören alle Gespräche und elektronische Kommunikation aus „dienstlichem Anlass“, die die Mitarbeiterin/der Mitarbeiter in Erfüllung des Arbeitsvertrags (oder des Dienstverhältnisses) für die Dienststelle führt. ³Mitarbeiter:innen können nicht verhindern, dass über die dienstliche E-Mail-Adresse private Nachrichten eingehen. ⁴Eingehende private Nachrichten sind umgehend zu löschen und aus dem Papierkorb zu entfernen.
- 8.2. ¹Nutzer:innen erhalten eine personalisierte LKI-Zugriffsberechtigung, wodurch gewährleistet wird, dass jede:r Nutzer:in einen persönlichen Zugriff auf die Dienste hat. ²Ein Zugriff auf das personenbezogene Postfach durch andere Personen ist grundsätzlich nicht erlaubt.

9. **Datenschutz und Datensicherheit**

- 9.1. ¹Beim Einrichten und Betreiben des LKI sind die datenschutzrechtlichen Vorschriften, insbesondere das Datenschutzgesetz der EKD und die Datenschutzverordnung der EKBO, einzuhalten. ²Verantwortliche im Sinne des Datenschutzes sind zuvorderst die jeweiligen Dienststellenleitungen. ³Die Anlage 2 – Katalog der Beschäftigtendaten und Schnittstellenverzeichnis legt eine abschließende Aufstellung fest, welche Beschäftigtendaten zu welchem Zweck an oder von welchem System übermittelt werden dürfen. ⁴Ebenso sind die im LKI genutzten Daten der Beschäftigten festgelegt.

- 9.2. ¹Es wird sichergestellt, dass die datenschutzrechtlichen Kontrollziele gemäß § 27 DSGVO-EKD wie insbesondere die Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Eingabekontrolle, Weitergabe sowie Auftrags- und Verfügbarkeitskontrolle effektiv realisiert werden. ²Die dazu getroffenen technischen und organisatorischen Maßnahmen (TOM) der Dienstleister werden mit den Verträgen zur Einsichtnahme für die HMAV und die Pfarrvertretung hinterlegt (3.3.). ³Eine Datenschutz-Folgenabschätzung gemäß § 34 DSGVO-EKD zum LKI wurde erstellt (Anlage 3). ⁴Die Stellungnahme des örtlich Beauftragten für den Datenschutz wird als Anlage 4 beigelegt.
- ⁵Die Verarbeitung personenbezogener Daten ist in Anlage 5 – Rechte- und Rollenkonzept festgelegt. ⁶Sie beinhaltet eine Darstellung von Zugriffsrechten auf personenbezogene Datenfelder, Funktionen und Auswertungen. ⁷Die personenbezogenen Datenfelder werden mit Angaben zur Bezeichnung und zum Inhalt des Datenfelds, zur Rechtsgrundlage oder Zweckbestimmung der Verarbeitung sowie zu Aufbewahrungszeiten und Löschfristen dokumentiert. ⁸Überdies sollten Datenfelder und Funktionen (Aktionen) aufgelistet werden, deren Bearbeitung personenbezogen gekennzeichnet wird (wie bei einer Änderungshistorie respektive einem Zeitstempel mit Nutzerkennung).
- ⁹Es wird gewährleistet, dass die Umsetzung der dokumentierten Maßnahmen jederzeit durch die oder den örtliche:n Beauftragte:n für den Datenschutz oder die HMAV überprüft werden kann.
- 9.3. ¹Die bei der Nutzung des LKI für Zwecke der Systemsicherheit und des ordnungsgemäßen Betriebs erfassten Benutzerdaten dürfen ausschließlich von den zugriffsberechtigten Personen für diese Zwecke verwendet werden. ²Zu anderen Zwecken dürfen die Daten nicht verwendet bzw. weitergegeben werden.
- 9.4. ¹Alle Personen, die Zugriff auf Beschäftigtendaten bzw. auf Auswertungen mit Beschäftigtenbezug erhalten, werden schriftlich gemäß § 26 DSGVO-EKD auf das Datengeheimnis verpflichtet. ²Diese Personen erhalten vorab eine Unterweisung in die Grundsätze des Datenschutzes durch den jeweiligen Arbeitgeber; das LKI-Team fragt dies vor der Einräumung der Rechte als Vertrauensinstanz ab. ³Weiteres regelt das Rechte- und Rollenkonzept.
- 9.5. ¹Auswertungen von personenbezogenen Daten zum Zwecke der Leistungs- und/oder der Verhaltenskontrolle von Mitarbeiterinnen und Mitarbeitern sind unzulässig. ²Widerrechtlich gewonnene Informationen unterliegen einem Beweisverwertungsverbot. ³Alle darauf gestützten arbeitsrechtlichen Maßnahmen sind unwirksam. ⁴Ein Verstoß gegen diese Bestimmungen kann arbeitsrechtliche bzw. dienstrechtliche Konsequenzen zur Folge haben.

9.6. ¹Der Zugriff auf personenbezogene LKI-Accounts darf nur in begründeten Fällen des Verdachts der missbräuchlichen Benutzung erfolgen. ²Liegt ein solcher Verdacht vor, wendet sich die Dienststellenleitung an die zuständige MAV und die LKI-Leitung. ³Die MAV informiert die HMAV und zieht ggf. eine Vertreterin oder einen Vertreter der HMAV zur Bewertung des Verdachtsfalles hinzu. ⁴Die Einsichtnahme unterliegt der Mitbestimmung durch die MAV. ⁵Die Einsichtnahme geschieht in einem gemeinsamen Termin der Dienststellenleitung oder der oder dem von ihr benannten Personalverantwortlichen der Dienststelle, der MAV und ggf. der HMAV, dem Datenschutzbeauftragten und einer Administratorin oder einem Administrator.

⁶Begründete Fälle sind insbesondere:

- dringender Verdacht einer schweren Amtspflicht- oder Arbeitsvertragsverletzung, die bei einmaliger Begehung oder im Wiederholungsfalle die Beendigung des Arbeitsverhältnisses oder die Einleitung eines Disziplinarverfahrens rechtfertigen würde, oder
- bei drohendem erheblichem Schaden für Dienststelle, Beschäftigte oder Dritte (z. B. Mobbing) oder
- Auffälligkeiten bei regelmäßigen Kontrollen bestimmter Bild/Video-Formate oder
- ggf. Key-Word-Liste.

⁷Eine personenbezogene Auswertung sollte möglichst im Beisein des Betroffenen stattfinden. ⁸Über die aus der Öffnung erworbenen Kenntnisse haben die Beteiligten Stillschweigen zu bewahren.

⁹Begründete Verdachtsfälle nach Satz 6 werden anonymisiert dokumentiert und alle drei Jahre evaluiert, ob dienststellenspezifische Häufungen auftreten oder ob das Verfahren richtig geregelt ist.

9.7. Personenbezogene Protokollierungen von Tätigkeiten sowie sonstige Kennzeichnungen von Daten und Dokumenten mit Informationen zur Identifikation der bearbeitenden Person (i. e. Protokollierung der letzten Bearbeitung oder Änderungshistorien) finden grundsätzlich nur statt, um rechtlichen Anforderungen zu genügen.

9.8. ¹Die Gewährleistung der Betroffenenrechte (Benachrichtigung, Auskunft, Korrektur, Sperrung, Löschung) ist vollumfänglich sicherzustellen. ²Den Beschäftigten wird auf Anfrage eine vollständige Auskunft bezüglich der zu ihrer Person gespeicherten Daten und Dokumente unentgeltlich zur Verfügung gestellt.

9.9. Das Konsistorium prüft, ob die Muster für die Nutzung privater Endgeräte für das LKI eine Präzisierung bedürfen, und stellt ggf. aktualisierte Muster zur Verfügung.

10. **Abwesenheit, Vertretung und Ausscheiden von Mitarbeiter:innen**

- 10.1.

1In Fällen geplanter längerer Abwesenheit (z. B. bei Urlaub, Kur, Weiterbildung) muss ein Abwesenheitsassistent durch die Mitarbeiterin oder den Mitarbeiter eingerichtet und aktiviert werden. 2Grundsätzlich erhält die genannte Vertretung keinen Zugriff auf das persönliche Postfach. 3Eine automatische Weiterleitung eingehender E-Mails ist aus Datenschutzgründen nicht erlaubt.
- 10.2.

1Für eine unvorhergesehene längere oder dauerhafte Dienstabwesenheit gilt Nr. 9.6. Sätze 2 bis 6 entsprechend. 2HMAV und Konsistorium gehen davon aus, dass Funktionspostfächer in zahlreichen Fällen Maßnahmen nach den vorstehenden Sätzen überflüssig machen, und empfehlen Dienststellen und Mitarbeitenden die Einrichtung von Funktionspostfächern.
- 10.3.

1In Fällen dauerhafter Abwesenheit (Ausscheiden aus dem Beschäftigungsverhältnis) ist der LKI-Account spätestens mit dem Datum des Ausscheidens durch die Vertrauensinstanz zu deaktivieren. 2Nach drei Monaten Inaktivität wird der LKI-Account gelöscht. 3Für diese Zeit ist vor Ausscheiden durch die Mitarbeiterin oder den Mitarbeiter selbständig der Abwesenheitsassistent zu aktivieren. 4Bei unplanmäßiger Abwesenheit geschieht dies (künftig) durch die Vertrauensinstanz auf Veranlassung durch die jeweilige Führungskraft (derzeit noch CANCOM, da weder Vertrauensinstanzen noch LKI-Team hierfür die erforderlichen Rechte haben).

11. **Seelsorge**

1Der Koordinierungsausschuss prüft, ob für Beschäftigte, deren Tätigkeiten, Informationen und Kommunikation unter das Seelsorgegeheimnisgesetz fallen (Beschäftigte nach § 3 Absatz 1 und 2 SeelGG), abweichende Regelungen notwendig sind. 2Hierbei sind die Vorschriften des Seelsorgegeheimnisgesetzes, des Datenschutzgesetzes (DSG.EKD) und des Kirchengesetzes zum Schutz vor sexualisierter Gewalt zu berücksichtigen.

12. **Schlussbestimmungen**

- 12.1. Die Anlagen 1 bis 5 sind Bestandteile dieser Dienstvereinbarung.
- 12.2. Änderungen, Ergänzungen oder Nebenabreden zu dieser Dienstvereinbarung bedürfen zu ihrer Gültigkeit der Schriftform.
- 12.3.

1Diese Dienstvereinbarung tritt am 1. Juni 2024 in Kraft und kann mit einer Frist von sechs Monaten zum Monatsende gekündigt werden. 2Bis zum Abschluss einer neuen Dienstvereinbarung wirken die Regelungen dieser Vereinbarung nach, jedoch längstens für ein Jahr.
- 12.4.

1Sollten einzelne Bestimmungen unwirksam sein oder werden, so berührt dies nicht die Fortgeltung dieser Vereinbarung im Übrigen. 2Die unwirksame Bestimmung ist durch eine wirksame Bestimmung zu ersetzen, die dem Sinn und Zwecke der

Dienstvereinbarung nach dem erkennbaren Willen der Vertragsparteien entspricht. ³Die Vertragsparteien verpflichten sich in diesem Fall zu sofortiger Verhandlungsaufnahme mit dem Ziel, die unwirksame Regelung einvernehmlich durch eine ihr in der Regelwirkung möglichst gleichkommende wirksame zu ersetzen. ⁴Gleiches gilt, wenn es zu Differenzen über die Auslegung kommen sollte.

- 12.5. Ist über einzelne Fragen dieser Dienstvereinbarung kein Einvernehmen zu erzielen, so entscheidet die Einigungsstelle.

Anlage 1 – Schulungskonzept

1. 1Das LKI-Team bietet monatlich mindestens eine Schulung an. 2Die Schulungen werden in der Regel online durchgeführt.
2. Die Schulungen werden in folgende Abschnitte zu je maximal 90 Minuten unterteilt:
 - a) Einführung (welche Funktionen gibt es überhaupt?),
 - b) Profil/Mein Konto/Prozesse im LKI (wie beantrage ich was etc.),
 - c) Mail,
 - d) Safe/Cloudspeicher,
 - e) weitere Funktionen.
3. Werden weitere Fachanwendungen eingebunden (z. B. für Meldewesen, Finanzwesen, Personalwesen,...), liegt die Schulungsverantwortung bei der Organisationseinheit, die die Fachanwendung verantwortet.
4. Bei Migrationen finden gesonderte Schulungen für die jeweilige, zu migrierende Organisationseinheit statt.
5. Nach jeder Schulung wird Feedback in geeigneter Weise eingeholt.
6. 1Die Hilfeseiten (Forum) im Landeskirchenweiten Intranet sind Teil des Schulungskonzeptes. 2Hier werden, in gesonderten Kategorien, insbesondere Anleitungen und Schulungsvideos zur Verfügung gestellt. 3Anleitungen und Schulungsvideos werden für zentrale Funktionen (Mail, Safe, Profil/Mein Konto) erstellt. 4Weitere Anleitungen und Schulungsvideos können auf Anfrage erstellt werden. 5Darüber hinaus dienen die Hilfeseiten (Forum) als Hilfe zur Selbsthilfe.
7. 1Für die Vertrauensinstanzen werden gesonderte Schulungen angeboten. 2Diese finden verpflichtend vor Aufnahme der Tätigkeit, nach größeren Systemanpassungen sowie bei Bedarf statt. 3Die Schulungen sind Arbeitszeit.

Anlage 2 – Katalog der Beschäftigtendaten**I. Pflichtdaten**

(um die eindeutige Identifizierung zu ermöglichen und doppelte Angaben auszuschließen)

- Anrede (m/w/keine Angabe),
- Vorname,
- Nachname,
- Geburtsjahr,
- Straße, Hausnummer,
- Postleitzahl,
- Stadt,
- Kontakt-E-Mail-Adresse (wird für den Registrierungsprozess benötigt und/oder für den Anmeldeprozess, wenn keine Mobilfunknummer hinterlegt wird),
- Kirchliche Organisationseinheit (Zugehörigkeit),
- Amt/Funktion,
- Berufsgruppe,
- Bezeichnung der Endgeräte (dienstlich/privat und Betriebssystem) auf die Mail oder Cloudspeicher synchronisiert werden

II. Freiwillige Angaben

- Foto,
- Mobilfunknummer (Achtung: ohne Telefonnummer sind Rücksetzprozesse komplizierter)

Anlage 3 und 4 – Vom Abdruck wird abgesehen

Anlage 5 – Rechte- und Rollenkonzept

Im Landeskirchenweiten Intranet der EKBO gibt es drei Rollen:

- a) Einzelnutzerinnen und Einzelnutzer,
- b) Master-Vertrauensinstanzen (LKI-Team),
- c) Vertrauensinstanzen.

a) **Einzelnutzerinnen und Einzelnutzer**

1. 1Aktuell stehen folgende Funktionen allen Nutzerinnen und Nutzern zur Verfügung: Mail, Cloudspeicher, Benutzerverwaltung (nur Zugriff auf die eigenen Kontoinformationen), EKBODialog, EKBOfairMeet, GMV, Umfragen, Hilfeforum, Computercheck, Bandbreitencheck. 2Darüber hinaus stehen entsprechend Berechtigten weitere Funktionen zur Verfügung (z. B. EKBO-Termine).
2. Die Nutzung des LKI setzt die Zustimmung zu den Nutzungsbedingungen und den AGB oder – bei beruflich Mitarbeitenden, in deren Dienststellen das LKI verbindlich eingesetzt wird – die Kenntnisnahme der Nutzungsbedingungen voraus.
3. 1Alle Nutzerinnen und Nutzer sind Einzelnutzerinnen oder Einzelnutzer. 2Sie registrieren sich für diejenige Organisationseinheit, in der sie ihre Hauptbeschäftigung ausüben. 3Ehrenamtliche registrieren sich für diejenige Organisationseinheit, in der sie überwiegend ehrenamtlich tätig sind. 4Das Hinzufügen weiterer Beschäftigungsverhältnisse ist möglich.

b) **Master-Vertrauensinstanzen**

1. Master-Vertrauensinstanzen haben folgende Aufgaben:
 - 1Sie können Benutzerkonten freischalten, sperren oder die Einrichtung ablehnen. 2Für Fachanwendungen gelten eigene Regelungen.
 - Die Master-Vertrauensinstanzen richten, in technischem Sinne, Vertrauensinstanzen für Kirchenkreise ein.
 - Die Master-Vertrauensinstanzen sind für die Schulung der Vertrauensinstanzen zuständig.
 - In technischem Sinne können Master-Vertrauensinstanzen die Vertrauensinstanzen in allen ihren Aufgaben unterstützen bzw. die Aufgaben stellvertretend für die Vertrauensinstanzen durchführen.
 - Die Master-Vertrauensinstanzen sind zuständig für nutzerbezogene Prozesse (Kontenfreischaltung u. ä.) im Bereich des Konsistoriums und der angeschlossenen Einrichtungen, soweit keine eigenen Vertrauensinstanzen vorhanden sind.

- Die Master-Vertrauensinstanzen dürfen alle technischen Maßnahmen selbstständig ergreifen, die in ihrem Aufgabenbereich zur Aufrechterhaltung und zur Sicherheit des Systems notwendig sind.
 - Die Master-Vertrauensinstanzen sind zuständig für die Erstellung von Schulungsvideos
2. ¹Die Sperrung von Benutzerkonten setzt voraus, dass der Nutzer oder seine Organisation erheblich gegen die Nutzungsbedingungen oder die Netiquette verstoßen hat. ²Dem Nutzer und der Organisation ist unverzüglich Gelegenheit zur Stellungnahme zu geben. ³Solange für das LKI keine eigene Netiquette in Kraft gesetzt wurde, gilt die Netiquette der Evangelischen Kirche Berlin-Brandenburg-schlesische Oberlausitz.
⁴Darüber hinaus können Nutzerkonten gesperrt werden, wenn Nutzer:innen bei der Registrierung Falschangaben bei den personenbezogenen Daten und/oder der Dienststelle sowie bei der Berufsgruppe gemacht haben.
⁵Die Sperrung erfolgt ebenso bei Ausscheiden aus dem ehren- und/oder hauptamtlichen Dienst.
 3. ¹Sie dürfen personenbezogene und/oder personenbeziehbare Daten oder Dateien aus einem Berechtigungskreis nicht in einen anderen übertragen und betriebliche oder persönliche Informationen nicht nach außerhalb ihres Arbeitsbereiches weitergeben, sofern dies nicht in dieser Dienstvereinbarung oder durch staatliche oder kirchliche Rechtsvorschrift geregelt ist. ²Dienstliche Anweisungen dieser Art sind nicht erlaubt und von den Master-Vertrauensinstanzen . ³Ausnahmen bedürfen der Zustimmung der HMAV. Eine Ausnahme kann nur erteilt werden, wenn die datenschutzrechtlichen Voraussetzungen erfüllt sind.
 4. ¹Die Master-Vertrauensinstanzen werden im Geschäftsverteilungsplan des Konsistoriums festgelegt; ist dies nicht der Fall, werden sie von der Leiterin oder vom Leiter des Referats IT beauftragt. ²Die Master-Vertrauensinstanzen werden der HMAV gegenüber benannt.

c) Vertrauensinstanzen

1. ¹Vertrauensinstanzen sind für die Benutzerverwaltung innerhalb eines Kirchenkreises, eines kirchlichen Verwaltungsamtes oder einer anderen eigenständigen Körperschaft (z. B. DWBO) zuständig. ²Sie erhalten zur Erfüllung ihrer Aufgaben Zugriff auf die unter I. und II. genannten Daten der Anlage [Katalog der Beschäftigtendaten]. ³Sie nehmen die unter c)3. genannten Aufgaben wahr.
2. Für die Benennung der Vertrauensinstanz ist der Kirchenkreis bzw. bei anderen Körperschaften die jeweilige Dienststellenleitung zuständig.
3. Die Vertrauensinstanzen sind zuständig für folgende Aufgaben:

- Freischaltung von Nutzerinnen und Nutzern für den Kirchenkreis, einschließlich seiner zugehörigen Kirchengemeinden, für den sie zuständig sind.
- Bewilligung und Wegnahme von besonderen Rechten (u. a. Alias-Adressen, Funktionspostfächer, Fachanwendungen) bezogen auf die Nutzerinnen und Nutzer für die sie zuständig sind.
- Sperrung und Löschung von Nutzerinnen und Nutzer im eigenen Zuständigkeitsbereich, wenn Sperrung bzw. Löschung geboten sind, von den Nutzerinnen und Nutzern aber nicht selbst initiiert werden.

II. Übersicht zu den Rechten in Bezug auf im LKI vorhandene Funktionen

Funktionen	Nutzer/in	Vertrauensinstanzen	Master-Vertrauensinstanz	Externe Dienstleister	Anmerkungen
Allgemein					
Erstellen und Verwalten von globalen Funktionen				x	Die im LKI zur Verfügung gestellten Funktionen werden in Absprache mit den beteiligten Landeskirchen festgelegt. Die Umsetzung und Verwaltung obliegt den jeweiligen Dienstleistern.
Inhalte melden	x	x	x		
Verwaltung von gemeldeten Inhalten				x	
Benutzerverwaltung					
Verwalten der Accounteinstellungen	x				Die Einstellungen des eigenen Accounts, inkl. Zugriff auf personenbezogene Daten wie Geburtsdatum, Anschrift etc. kann nur der/die Nutzer:in verwalten.

Funktionen	Nutzer/in	Vertrauensinstanzen	Master-Vertrauensinstanz	Externe Dienstleister	Anmerkungen
Ansicht von Benutzerprofilen, inkl. Angabe zu Nutzernamen, Registrierungsdatum, angebundene Endgeräte, bewilligte Fachanwendungen, Aliasadressen, zugeordnete Funktionspostfächer, Beschäftigungsverhältnisse, Kontostatus, Speicherplatzverbrauch		x (nur das Profil derjenigen Nutzer:innen für deren Organisationseinheit sie zuständig sind)	x (alle)	x	Die Ansicht beinhaltet keine personenbezogenen Daten wie Kontakt-E-Mail-Adresse, Geburtsdatum, Anschrift oder Telefonnummer.
Hinzufügen weiterer Beschäftigungsverhältnisse	x (nur das jeweils eigene Profil)	x (nur für das Profil derjenigen Nutzer:innen für deren Organisationseinheit sie zuständig sind)	x (alle)		
Cloudspeicher					
Anlage von Organisationscloudspeichern (Departments)	x				Prozessgesteuert: Nutzer:innen können einen OCS beantragen. Dieser

Funktionen	Nutzer/in	Vertrauensinstanzen	Master-Vertrauensinstanz	Externe Dienstleister	Anmerkungen
					Antrag muss von der Vertrauensinstanz bestätigt werden. Der/die beantragende Nutzer:in wird Eigentümer:in des OCS und vergibt im Anschluss daran Lese- und/oder Schreibrechte für die Inhalte des OCS.
Zugriff auf Inhalte des OCS (Department)	(x)				Alle Nutzer:innen, denen die entsprechende Rechte von den Eigentümer:innen eingeräumt wurden.
Zugriff auf persönlichen Cloudspeicher	x				
öffentliche Links erstellen	x				Bei eigenen Dokumenten/Ordern und bei OCS-Daten soweit und insofern dafür die entsprechenden Rechte von den Eigentümer:innen des OCS eingeräumt wurden.

Funktionen	Nutzer/in	Vertrauens- instanzen	Master- Vertrauens- instanz	Externe Dienstleis- ter	Anmerkungen
Besitzer:in zu OCS hinzufügen	(x)	x	x	x	Im Falle der Einzelnutzer:innen nur der/die Eigentümer:in des OCS. VI, Master-VI und Dienstleister können Eigentümer:innen hinzufügen, haben aber keinen Zugriff auf die Inhalte des OCS.
Besitzer:in aus OCS entfernen	(x)	x	x	x	Im Falle der Einzelnutzer:innen nur der/die Eigentümer:in des OCS. VI, Master-VI und Dienstleister können Eigentümer:innen entfernen, haben aber keinen Zugriff auf die Inhalte des OCS.
E-Mail					
Zugriff auf das eigene Postfach	x				
Alias beantra- gen	x				
Funktionspost- fach beantragen	x				

Funktionen	Nutzer/in	Vertrauensinstanzen	Master-Vertrauensinstanz	Externe Dienstleister	Anmerkungen
Zugriff auf Funktionspostfach	(x)				Alle Nutzer:innen, denen von der/dem Besitzer:in des Postfachs die entsprechenden Rechte eingeräumt wurden.
Besitzer hinzufügen	(x)	x	x	x	Im Falle der Einzelnutzer:innen nur der/die Besitzer:in des Postfachs. VI, Master-VI und Dienstleister können Besitzer:innen für Funktionspostfächer hinzufügen, haben aber keinen Zugriff auf die Inhalte des Postfachs.
Besitzer entfernen	(x)	x	x	x	Im Falle der Einzelnutzer:innen nur der/die Besitzer:in des Postfachs. VI, Master-VI und Dienstleister können Besitzer:innen für

Funktionen	Nutzer/in	Vertrauensinstanzen	Master-Vertrauensinstanz	Externe Dienstleister	Anmerkungen
					Funktionspostfächer entfernen, haben aber keinen Zugriff auf die Inhalte des Postfachs
Kalender					
Erstellen von Terminen	x				Jeweils im eigenen Kalender; bei Funktionspostfächern alle, denen die entsprechenden Rechte eingeräumt wurden.
Einladung zu Terminen					Jeweils im eigenen Kalender; bei Funktionspostfächern alle, denen die entsprechenden Rechte eingeräumt wurden.
Löschen von Terminen					Jeweils im eigenen Kalender; bei Funktionspostfächern alle, denen die entsprechenden Rechte eingeräumt wurden.
Zugriff auf eigenen Kalender	x				

Funktionen	Nutzer/in	Vertrauensinstanzen	Master-Vertrauensinstanz	Externe Dienstleister	Anmerkungen
Zugriff auf die Frei/Gebucht-Ansicht von anderen Nutzer:innen im System	x	x	x		
EKBODialog					
Chat starten	x				
Kanal eröffnen	x				
Zugriff auf die eigenen Chatinhalte	x				
Zugriff auf Statistiken			x	x	
Zugriff auf Adminbereich			x	x	
EKBOfairMeet					
Videomeeting starten	x				
OTRS (Ticketsystem für VI und MVI)					Im OTRS laufen die meisten prozessgesteuerten Anträge ein.
Nutzer:innen freischalten		x (nur diejenigen Nutzer:innen, die sich für jene Organisationseinheit registrieren, für die die VI zuständig ist)	x (alle)	x	

Funktionen	Nutzer/in	Vertrauensinstanzen	Master-Vertrauensinstanz	Externe Dienstleister	Anmerkungen
Nutzer:innen ablehnen		x (nur diejenigen Nutzer:innen, die sich für jene Organisationseinheit registrieren, für die die VI zuständig ist)	x (alle)	x	
Zugriff auf Nutzer:innendaten, die im Registrierungsprozess angegeben werden		x (nur diejenigen Nutzer:innen, für deren Organisationseinheit die VI zuständig ist)	x (alle)	x	Beinhaltet auch die personenbezogenen Daten wie Geburtsdatum, Anschrift etc. Ausnahme: hinterlegte Mobilfunknummer. Diese kann ausschließlich von den Nutzer:innen selbst eingesehen werden.
Bewilligung von Anträgen (z. B. Alias)		x (nur diejenigen Nutzer:innen, für deren Organisationseinheit die VI zuständig ist)	x (alle)	x	

Funktionen	Nutzer/in	Vertrauensinstanzen	Master-Vertrauensinstanz	Externe Dienstleister	Anmerkungen
Ablehnung von Anträgen (z. B. Alias)		x (nur diejenigen Nutzer:innen, für deren Organisationseinheit die VI zuständig ist)	x (alle)	x	

