Az. 82/10-29

Dienstvereinbarung zur Einführung und Anwendung des Systems Microsoft 365[1]

Die Evangelisch-Lutherische Kirche in Bayern, vertreten durch den Leiter des Landeskirchenamtes, Herrn Oberkirchenrat Dr. Nikolaus Blum, den Leiter der Gemeindeabteilung im Landeskirchenamt, Herrn Oberkirchenrat Professor Dr. Hans-Peter Hübner und den Leiter des Kompetenzzentrums CEO, Herrn Markus Bönisch

und

der Gesamtausschuss Kirche der Mitarbeitervertretungen in der ELKB, vertreten durch den Vorsitzenden, Herrn Markus Noll (GA Kirche)

schließen gemäß §§ 4 Abs. 3 AGMVG, 54 Abs. 2 MVG-EKD i. V. m. §§ 36, 40 h, i und j MVG-EKD folgende

Dienstvereinbarung zur Einführung und Anwendung des Systems Microsoft 365

Präambel

Die Anwendungen von Microsoft 365 stellen wesentliche Informations- und Kommunikationsmedien der modernen Arbeitswelt dar. Mit der Nutzung sind allerdings auch Risiken verbunden. Insbesondere durch die neue Cloud-basierte Anwendung sind mannigfaltige Überwachungsszenarien möglich. Um die Interessen des Dienstgebers an der Bereitstellung moderner und effizienter Arbeits- und Kommunikationsmittel und das Recht der Beschäftigten auf informationelle Selbstbestimmung in Einklang zu bringen und die Beschäftigten vor einer über die Regelungen dieser DV hinausgehenden Leistungs- und Verhaltenskontrolle zu schützen, wird die folgende Dienstvereinbarung geschlossen.

§ 1
Gegenstand der Vereinbarung

(1) Die Dienstvereinbarung regelt die Einführung und Anwendung von Microsoft 365. Sie regelt dabei insbesondere, welche der von Microsoft 365 umfassten Einzelprogramme (im Folgenden: Anwendungen) zur Anwendung kommen können.

(2) Alle zulässigen und freigegebenen Anwendungen von Microsoft 365 (z.B. Exchange Online, Sharepoint Online, Teams, Skype for Business Online, OneDrive Business, Planner, Delve etc.) werden in Anlage 1 zu dieser Dienstvereinbarung abschließend aufgeführt. Alle weiteren Anwendungen werden deaktiviert und dürfen nur nach schriftlicher Vereinbarung mit dem GA Kirche genutzt werden.

[1] Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung der Sprachformen männlich, weiblich und divers (m/w/d) verzichtet.

(3) In Anlage 1 dieser Dienstvereinbarung sind auch zu dokumentieren:

a) Alle zulässigen bzw. freigegebenen Anwendungen und Komponenten aus dem Bereich Sicherheit und Compliance.[2]
b) Mit Hilfe von Microsoft 365 erstellte unternehmensspezifische Anwendungen, die Beschäftigtendaten verarbeiten.[3]
c) Externe und verbundene Anwendungen oder Dienste, die in Microsoft 365-Anwendungen eingebunden werden und Beschäftigtendaten verarbeiten.

(4) Soweit eine Partei dies verlangt, wird für eine in Anlage 1 aufgeführte Anwendung von Microsoft 365 eine ergänzende Vereinbarung in Anlage 2 abgeschlossen. Die Parteien können dabei konkrete Einzelregelungen für jede Anwendung treffen. Anlage 2 enthält zumindest:

a) Eine kurze, prägnante Beschreibung der Funktion, Verarbeitung von Beschäftigtendaten (Zweckbestimmung, zulässige Kategorien von Beschäftigtendaten, zulässige Auswertungen von Beschäftigtendaten).
b) Vorgaben zur Nutzung im Unternehmen.
c) Ein Berechtigungskonzept, soweit dieses über das generelle Berechtigungskonzept zu MS 365 hinausreicht.
d) Fristen und Kriterien zur Löschung von Beschäftigtendaten.

§ 2
Geltungsbereich

Diese Dienstvereinbarung gilt in persönlicher Hinsicht für alle Beschäftigten der Evangelisch-Lutherischen Kirche in Bayern und ihrer Gliederungen (Art. 2 Kirchenverfassung), die in den Zuständigkeitsbereich des Gesamtausschusses Kirche fallen, mit Ausnahme der Dienststellenleitungen im Sinne von § 4 MVG-EKD.

§ 3
Definitionen

(1) Es gelten die technischen und organisatorischen Maßnahmen (TOMs) im Sinne des § 27 EKD-Datenschutzgesetz (DSG-EKD). Diese sind in der Datenschutzfolgeabschätzung beschrieben, die im Intranet der Landeskirche veröffentlicht ist.

(2) Eine Schnittstelle (engl.: interface) ist ganz allgemein die Verbindungsstelle zwischen zwei miteinander in Beziehung stehenden informationsverarbeitenden Systemen oder Systemkomponenten, über die der Austausch von Daten oder Steuerinformationen erfolgt.

(3) Administrative Zwecke sind Zwecke zur Sicherstellung des ordnungsgemäßen Betriebs.

[2] Z.B. Azure Active Directory, Azure Information Protection, Data Loss Prevention, eDiscovery, Intune etc.
[3] Z.B. über Sharepoint Online oder PowerApps.

§ 4
Zulässige Verarbeitung von Beschäftigtendaten

(1) Die Verarbeitung von Beschäftigtendaten durch Microsoft 365 ist ausschließlich im Rahmen dieser Dienstvereinbarung sowie ihrer Anlagen zulässig.

(2) Die Verarbeitung von Beschäftigtendaten durch Microsoft 365 ist nur zulässig, soweit dies zur Erfüllung der folgenden Zwecke erforderlich ist:

a) Zur Unterstützung der Kommunikation sowie der Zusammenarbeit in Gruppen bzw. Teams.
b) Zur Umsetzung und Kontrolle von Datenschutz und IT-Sicherheit.
c) Zur Dokumentation des zuständigen Bearbeiters, um Rückfragen und Verantwortlichkeiten im Einzelfall zu klären.

Weitere zulässige Zwecke können in den ergänzenden Regelungen zu einzelnen Anwendungen von Microsoft 365 in Anlage 2 festgelegt werden.

(3) Es dürfen ausschließlich die folgenden Kategorien von Beschäftigtendaten mit Microsoft 365 verarbeitet werden:

a) Benutzerkennungen, Passwörter, Zugriffsrechte und Rollen.
b) Daten des Microsoft 365-Überwachungsprotokolls der Benutzer.
c) Portraitbild für das Benutzerprofil bei Einwilligung des betreffenden Beschäftigten.

Weitere zulässige Kategorien von Beschäftigtendaten können in den ergänzenden Regelungen zu einzelnen Anwendungen von Microsoft 365 in Anlage 2 festgelegt werden.

(4) Auswertungen und Reports mit Beschäftigtendaten dürfen nur verarbeitet werden, soweit dies durch diese Dienstvereinbarung und ihre Anlagen ausdrücklich zugelassen wird. Zulässige Auswertungen von Beschäftigtendaten können in den ergänzenden Regelungen zu einzelnen Anwendungen von Microsoft 365 in Anlage 2 festgelegt werden. Alle anderen möglichen, aber nicht zugelassenen automatisierten Auswertungen sind, soweit technisch möglich, zu deaktivieren oder durch entsprechende Berechtigungsvergabe zu sperren.

(5) Im Übrigen orientiert sich die Datenverarbeitung an den Grundsätzen des EKD-Datenschutzgesetzes (DSG-EKD) und der Datenschutzausführungsverordnung (AVDSG); insbesondere im Hinblick auf den Grundsatz der Datenminimierung. Beschäftigtendaten sind weitestgehend, soweit technisch möglich, zu anonymisieren bzw. zu pseudonymisieren.

(6) Administratoren verpflichten sich, personenbezogene Daten selbst nicht ohne Befugnis zu verarbeiten und anderen Personen diese Daten nicht unbefugt mitzuteilen oder zugänglich zu machen. Sie werden insbesondere verpflichtet, die datenschutzrechtlichen Vorgaben und Weisungen im Unternehmen zu beachten.

§ 5
Spezifische Microsoft 365 Regelungen

(1) Microsoft 365 erstellt über die Anwendungen ein automatisiertes Überwachungsprotokoll (Audit Log)[4]. Eine Auswertung des Audit Logs erfolgt nur zu Administrationszwecken sowie zur Kontrolle von Datenschutz und IT-Sicherheit. Das Audit Log wird für eine maximale Dauer von 180 Tagen gespeichert. Export und externe Speicherung der Daten aus dem Audit Log sind unzulässig.

(2) Aktivitäten-Berichte (Usage Reports) speichern einen rückwärtigen Zeitraum von maximal 180 Tagen. Die Auswertung der Berichte erfolgt nur für administrative Zwecke durch die Administratoren, soweit sie nur zusammengefasste oder benutzerbezogene Daten über Nutzungshäufigkeiten und Ressourcenverbrauch enthalten. Abweichende Regelungen für einzelne Microsoft 365- Anwendungen gehen vor.

(3) Enthält eine Anwendung die Funktion einer Verfügbarkeitsanzeige (z.B. „verfügbar“, „beschäftigt“ etc.), so ist der Status für jeden Benutzer steuerbar. Es erfolgt keine Aufzeichnung der Verfügbarkeitsanzeige.

(4) Die mobile Nutzung von Microsoft 365 Anwendungen über mobile Endgeräte wie Smartphone, Tablets ist nur nach Vereinbarung ergänzender Regelungen in Anlage 3 möglich.

(5) Nutzung von Office Graph und Delve

a) Die Nutzung von Office Graph über die Graph-API-Schnittstelle ist ausgeschlossen.
b) Delve wird für sämtliche Beschäftigten deaktiviert und erst nach ergänzender Vereinbarung in Anlage 2 zu dieser Dienstvereinbarung zur Nutzung freigegeben.

(6) Die Übermittlung von Nutzungsdaten zur Produktverbesserung an Microsoft wird im Rahmen der technischen Möglichkeiten deaktiviert.

(7) Es werden keine Workplace-Analytics-Funktionen bereitgestellt oder genutzt. Ebenso werden keine myAnalytics-Funktionen bereitgestellt oder genutzt. Insbesondere werden keine Auswertungen über Beziehungen, z. B. Beziehungsgrafiken, erstellt.

(8) Die Funktionsbereiche von Security & Compliance dürfen ausschließlich zu folgenden Zwecken genutzt werden:

a) Gewährleistung der Systemsicherheit,
b) Nicht-personalisierte Feststellung der Nutzungsdauer und -häufigkeit,
c) Analyse und Korrektur von technischen Fehlern im System,
d) Optimierung der IT-Systeme,
e) statistische Auswertungen ohne individuelle Kennung,
f) Missbrauchskontrolle.

[4] Dieses umfasst die Protokollierung aller Aktivitäten von Benutzern und Administratoren, auch bezüglich Änderungen von Konfigurationseinstellungen, Berechtigungsvergabe etc.

§ 6
Schnittstelle zu anderen Systemen

(1) Microsoft 365 ermöglicht Schnittstellen, über welche Beschäftigtendaten von anderen IT-Systemen in Microsoft 365 eingespeist werden oder von Microsoft 365 an andere IT-Systeme übergehen.

(2) Sämtliche Schnittstellen werden in Anlage 4 dieser Dienstvereinbarung unter Angabe der übergehenden Datenkategorien sowie des Zwecks der Verarbeitung in anderen Systemen dokumentiert.

§ 7
Aufbewahrungs- und Löschfristen

(1) Der datenschutzrechtlich Verantwortliche sorgt für die Einhaltung der gesetzlichen Aufbewahrungsfristen.

(2) Vorgaben zur Umsetzung der Löschfristen bzw. Löschkriterien (z.B. Zuständigkeiten für Umsetzung und Überwachung) legt der Dienstgeber in einem geeigneten Löschkonzept fest.

§ 8
Datentransfer an Dritte

(1) Soweit durch Microsoft 365 die Verarbeitung von Beschäftigtendaten im Wege der Auftragsverarbeitung nach § 30 EKD-Datenschutzgesetz (DSG-EKD) erfolgt, prüft der datenschutzrechtlich Verantwortliche im Vorfeld der Verarbeitung gem. § 27 DSG-EKD sämtliche erforderlichen technischen und organisatorischen Sicherheitsmaßnahmen (TOMs). Er nimmt ferner eine datenschutzrechtliche Risikoanalyse nach Maßgabe von § 34 DSG-EKD und eine Datenschutzfolgenabschätzung (DSFA) vor. Der GA Kirche erhält auf Anforderung jeweils eine Kopie über die Dokumentation der TOMs sowie ggf. über das Ergebnis der DSFA (ggf. mit Stellungnahme des Datenschutzbeauftragten).

(2) Die Parteien legen in Anlage 5 dieser Dienstvereinbarung ein allgemeines Rollen- und Berechtigungskonzept fest. Dieses regelt insbesondere:

a) Die Zugriffsrechte und Rollen, soweit diese Benutzer Zugriff auf Daten von Beschäftigten im Geltungsbereich erhalten.
b) Die Zugriffsrechte von Administratoren.

Soweit spezielle Zugriffsrechte für einzelne Microsoft 365 Anwendungen in Anlage 2 festgelegt werden, gelten diese vorrangig und sind im Berechtigungskonzept zu übernehmen.

(3) Dem GA Kirche sind alle Verträge mit Auftragsverarbeitern gemäß § 30 DSG-EKD (Software-Anbieter, Cloud Anbieter, Wartungsunternehmen, Server-Betreiber etc.)

vorzulegen. Sofern die Datenübermittlung in ein Drittland auf Grundlage von § 30 Abs. 2 i. V. m. § 10 DSG-EKD erfolgt, hat der Dienstgeber dem GA Kirche geeignete Garantien zur Datenübermittlung nachzuweisen.

(4) Der Dienstgeber kontrolliert regelmäßig, mindestens zweijährlich, die Einhaltung dieser Dienstvereinbarung sowie die Einhaltung der sonstigen Datenschutzvorschriften, insbesondere der TOMs (entsprechend § 27 DSG-EKD). Dem GA Kirche ist unverzüglich eine Kopie des jeweiligen Prüfberichts vorzulegen. Der GA Kirche kann zu jeder jährlichen Prüfung eigene Prüffragen einreichen, die zu berücksichtigen sind.

§ 9
Leistungs- und Verhaltenskontrollen

(1) Eine generelle Überwachung sowie eine Leistungs- oder Verhaltenskontrolle finden nicht statt.

(2) Ergibt sich ein begründeter Verdacht auf eine unberechtigte oder missbräuchliche Nutzung von Microsoft 365, einer strafbaren Handlung oder eines sonstigen Vergehens oder schwerwiegender Arbeitspflichtverletzung, erhält der Dienstgeber nach vorheriger Zustimmung der örtlichen Mitarbeitervertretung unter Hinzuziehung eines Mitgliedes der örtlichen Mitarbeitervertretung und des betrieblichen Datenschutzbeauftragten Zugriff auf die Protokolldaten, die zur Aufklärung des Verdachts erforderlich sind.

(3) Die Möglichkeit einer Kontrolle aufgrund der gesetzlichen Vorschriften, insbesondere aufgrund von § 49 Abs. 2 DSG-EKD, bleiben unberührt.

§ 10
Rechte des GA Kirche

(1) Der GA Kirche hat das Recht, die Einhaltung dieser Dienstvereinbarung unter Wahrung der Persönlichkeitsrechte der Dienstnehmer auf begründeten Anlass hin zu überprüfen.

(2) Der GA Kirche kann zur Durchführung seiner aus dieser Dienstvereinbarung resultierenden Aufgaben nach Abstimmung mit dem Dienstgeber einen Sachverständigen seiner Wahl hinzuziehen; die notwendigen Kosten trägt nach vorheriger Abstimmung der Dienstgeber (§ 30 Abs. 2 MVG-EKD).

(3) Dem GA Kirche sind, soweit nicht anders geregelt, auf Anforderung alle erforderlichen Unterlagen zur Erfüllung seiner Pflichten und Ausübung seiner Rechte zur Verfügung zu stellen.

(4) Der GA Kirche ist über festgestellte unzulässige Datenverarbeitungen mit Microsoft 365 sowie über Meldepflichten nach §§ 32, 33 DSG-EKD zu informieren. Der GA Kirche hat bei unzulässigen Verarbeitungen von Beschäftigtendaten ein Vetorecht. Betreffende Verarbeitungen sind soweit technisch möglich zu deaktivieren oder durch andere geeignete Maßnahmen zu unterbinden.

(5) Der GA Kirche kann einzelne GA Mitglieder zu Qualifizierungsmaßnahmen entsenden.

§ 11
Software-Updates und Änderungen

(1) Der GA Kirche ist regelmäßig über die wesentlichen Änderungen und Erweiterungen von Microsoft 365 entsprechend den Release-Notes und der Roadmap des Software-Herstellers zu informieren. Dies gilt nicht für rein technische Änderungen anlässlich von Fehlerkorrekturen, Usability-Verbesserungen oder Performance-Verbesserungen.

(2) Änderungen oder Erweiterungen, die zu Abweichungen von den Vorgaben dieser Dienstvereinbarung und ihrer Anlagen führen, insbesondere bzgl. der vereinbarten Anwendungen, Datenkategorien oder Auswertungen, des Berechtigungskonzepts sowie der technischen und organisatorischen Maßnahmen der Datensicherheit, unterliegen der Mitbestimmung des GA Kirche.

§ 12
Schlussbestimmungen

(1) Diese Dienstvereinbarung tritt am 1. Februar 2022 in Kraft.

(2) Sie kann von beiden Vertragspartnern mit einer Frist von zwölf Monaten zum Jahresende gekündigt werden.

(3) Eine diese Dienstvereinbarung ersetzende Vereinbarung soll bis zum Ablauf der Kündigungsfrist erstellt werden.

(4) Die Anlagen sind Bestandteil der Dienstvereinbarung:

- Anlage 1: Alle zulässigen und freigegebenen Anwendungen von Microsoft 365
- Anlage 2: Ggf. im Laufe der Zeit noch zu schließende ergänzende Regelungen/ Vereinbarungen zu einzelnen in Anlage 1 benannten Anwendungen
- Anlage 3: Vereinbarung über ergänzende Regelungen zur mobilen Nutzung von Microsoft 365- Anwendungen über mobile Endgeräte gemäß § 5 Abs. 4 DV Microsoft 365
- Anlage 4: Dokumentation sämtlicher Schnittstellen gemäß § 6 Abs. 2 DV Microsoft 365
- Anlage 5: Allgemeines Rollen- und Berechtigungskonzept gemäß § 8 Abs. 2 DV Microsoft 365

München, 28.02.2022	München, 04.03.2022	München, 28.02.2022
Ort, Datum	Ort, Datum	Ort, Datum
Gez.	Gez.	Gez.
Dr. Nikolaus Blum	Prof. Dr. Hans-Peter Hübner	Markus Bönisch

Hof, den 04.03.2022

Gez.

Markus Noll

Leistungsspektrum **Anlage 1**

	Leistung	Exchange Nutzer	Teams und Exchange Nutzer	AHP Nutzer inkl. Exchange und Teams	Klassischer Arbeitsplatz mit Exchange und Teams (mit Scan to Mail / ohne Scan to Folder)	Ehrenamt mit Exchange und Teams
1.	**Grundpakete**					
1.1.	CANCOM AHP (virtueller Arbeitsplatz)	nicht enthalten	nicht enthalten	x	nicht enthalten	nicht enthalten
1.2.	Microsoft Lizenz	Exchange Online Plan	Office 365 E1	Microsoft 365 E3	Office 365 E3	Office 365 F3
1.3.	Supportleistung durch CANCOM	Exchange/E-Mail	Exchange/E-Mail	vollumfänglich	Exchange/E-Mail	Exchange/E-Mail
2.	**Softwareprodukte**					
	Microsoft 365 Apps for Enterprise					
2.1.	PowerPoint	nicht enthalten	nur online/Mobile	x	x	nur online/Mobile
2.2.	Word	nicht enthalten	nur online/Mobile	x	x	nur online/Mobile
2.3.	Excel	nicht enthalten	nur online/Mobile	x	x	nur online/Mobile
2.4.	OneNote	nicht enthalten	nur online/Mobile	x	x	nur online/Mobile
2.5.	Publisher	nicht enthalten	nicht enthalten	x	x	nicht enthalten
2.6.	Access	nicht enthalten	nicht enthalten	x	x	nicht enthalten
2.7.	Outlook	nicht enthalten	nur online/Mobile	x	x	nur online/Mobile
	E-Mail, Kalender und Adressbuch					
2.8.	Outlook Web Access	enthalten, Kosten werden von der Landeskirche übernommen				
2.9.	Exchange	enthalten, Kosten werden von der Landeskirche übernommen				
	Besprechung und Anrufe					
2.10.	Teams [1)]	nicht enthalten	x	x	x	x
	Soziales Netzwerk und Intranet					
2.11.	SharePoint Online	nicht enthalten	x	x	x	x
	Dateien und Inhalte					
2.12.	OneDrive for Business	nicht enthalten	x	x	x	x
2.13.	Geräte- und Anwendungsverwaltung (Service nicht freigeschaltet)	nicht enthalten	nicht enthalten	x	nicht enthalten	nicht enthalten
2.14.	Windows Enterprise (nicht zentral konfiguriert)	nicht enthalten	nicht enthalten	x	nicht enthalten	nicht enthalten
2.15.	Identitätsmanagement (enthalten in AADP1; Identity Manager)	nicht enthalten	nicht enthalten	x	nicht enthalten	nicht enthalten
2.16.	Zugriffsmanagement (enthalten in AADP1)	nicht enthalten	nicht enthalten	x	nicht enthalten	nicht enthalten
	Bedrohungsschutz					
2.17.	Microsoft Advanced Threat Analytics	nicht enthalten	nicht enthalten	x	nicht enthalten	nicht enthalten
2.18.	Windows Defender Antivirus und Device Guard	nicht enthalten	nicht enthalten	x	nicht enthalten	nicht enthalten
2.19.	Microsoft Defender für Office 365 Plan 1	enthalten, Kosten werden von der Landeskirche übernommen				

2.20.	Azure Information Protection Plan 1 (Informationsschutz)	enthalten, Kosten werden von der Landeskirche übernommen				
3.	**Inkludierter Online-Speicherplatz**					
3.1.	Exchange Online (Postfach)	100 GB	50 GB	100 GB	100 GB	2 GB
3.2.	OneDrive for Business (persönlicher Speicher)	nicht enthalten	1 TB	5 TB	5 TB	2 GB
3.3.	SharePoint Online (geteilter Speicher)	nicht enthalten	1 TB	unlimitiert	unlimitiert	nur Nutzer
4.	**Backup**	enthalten, Kosten werden von der Landeskirche übernommen	zusätzlich	zusätzlich	zusätzlich	zusätzlich
5.	**Optionale Lizenzen**					
5.1.	Visio Online Plan 1	zusätzlich	zusätzlich	zusätzlich	zusätzlich	zusätzlich
5.2.	Visio Online Plan 2	zusätzlich	zusätzlich	zusätzlich	zusätzlich	zusätzlich
5.3.	Project Online Essentials	zusätzlich	zusätzlich	zusätzlich	zusätzlich	zusätzlich
5.4.	Project Plan 3	zusätzlich	zusätzlich	zusätzlich	zusätzlich	zusätzlich
5.5.	Project Plan 5	zusätzlich	zusätzlich	zusätzlich	zusätzlich	zusätzlich
5.6.	Soluzione Lernwelt	nicht enthalten	zusätzlich	zusätzlich	zusätzlich	zusätzlich
6.	**Hotline (derzeit nur für Exchange)**	0911/6419496513	0911/6419496513	0911/6419496513	0911/6419496513	0911/6419496513
7.	**Hardware-/Softwareempfehlungen**					
7.1.	Erforderliches Betriebssystem	entfällt	entfällt	Windows 10 Pro	entfällt	entfällt
7.2.	Microsoft Team unter Windows 10	entfällt	i5 8. Generation+ / 8GB RAM / SSD	i5 8. Generation+ / 8GB RAM / SSD	i5 8. Generation+ / 8GB RAM / SSD	i5 8. Generation+ / 8GB RAM / SSD
8.	**Einbindung von Zoom über Connect4Video**	nicht enthalten	nicht enthalten	X	nicht enthalten	nicht enthalten

[1)] Dies umfasst MS Teams und alle datenschutzrechtlich zugelassenen Apps wie z.B. Planner

Version 1, Stand 12.1.2022

Anlage 2

1. Regelungen für die Nutzung von Videokonferenzen

Zur Information: Der Gesamtausschuss Kirche hat der dienstlichen Nutzung der Video-Chat-Plattform „Zoom“ am 14. Mai 2020 unter folgenden Maßgaben zugestimmt:

- Beweisverwertungsverbot für Personalmaßnahmen, Verbot zur Nutzung von Verhaltens- und Leistungskontrolle,
- Gestattung von Aufzeichnungen nur nach ausdrücklicher Zustimmung aller Teilnehmenden an der jeweiligen Videokonferenz bei entsprechender Anpassung der vorbelegten Datenschutzeinstellungen,
- Beschaffung und Nutzung der Zoom-Lizenzen nur über den Rahmenvertrag mit der ELKB bei der Fa. Connect4Video GmbH.

Für die Nutzung von Videokonferenzen mit „MS Teams“ gelten folgende Kriterien:

- Beweisverwertungsverbot für Personalmaßnahmen, Verbot zur Nutzung von Verhaltens- und Leistungskontrolle,
- Gestattung von Aufzeichnungen nur nach ausdrücklicher Zustimmung aller Teilnehmenden an der jeweiligen Videokonferenz,
- Anpassung der vorbelegten Datenschutzeinstellungen auf den vorigen Punkt;
- Beschaffung und Nutzung der MS 365 Lizenzen nur über den ELKB-Tenant bei Microsoft.

Aufgrund der aktuellen technischen Gestaltung werden nachfolgend die Nutzungsmöglichkeiten der beiden Systeme exemplarisch dargestellt.

2. a) Legende

Für diese Form der Videokonferenz und den damit verbundenen Austausch von Informationen ist diese Anwendung geeignet.	
Für diese Form der Videokonferenz und den damit verbundenen Austausch von Informationen ist diese Anwendung **NICHT** geeignet.	

2. b) Szenarien

Beispiel-Nr.	Beispiele zum Einsatz eines Videokonferenzsystems	Zoom	Teams
1	Vorbereitung oder weiteren Bearbeitung eines Projektes. Bei der Projektarbeit werden Informationen zum Auf- und Ausbau des Projekts ausgetauscht und die Kommunikation bezieht sich lediglich auf den projektbezogenen Sachverhalt.		
2	Vorbereitung einer Veranstaltung und den dazugehörigen organisatorischen Rahmenbedingungen (bspw. zeitlicher Ablauf, Einsatz von Personen, inhaltliches Programm etc.).		
3	Fachlicher Austausch von Informationen zu ausgesuchten Themen.		
4	Austausch von persönlichen Informationen im Rahmen von seelsorgerlichen Gesprächen.		
5	Gespräche bspw. von Klienten, Patienten oder andere Schutzbedürftige.		
6	Gespräche mit Behörden zur Betreuung von Klienten oder andere Schutzbedürftige.		
7	Gespräche mit Mitarbeiter*innen zum Leistungsstand, zur Zufriedenheit am Arbeitsplatz o.ä.		
8	Treffen von Arbeitsgruppen zum Austausch diverser arbeitsbezogener Themen.		
9	Gespräche im Rahmen eine betrieblichen Eingliederungsmanagements (BEM)		

Beispiel-Nr.	Beispiele zum Einsatz eines Videokonferenzsystems	Zoom	Teams
10	Arbeit der Mitarbeitervertretung		

3. Ergänzende Hinweise

Hingewiesen wird auf:

- den im Zusammenhang mit dem Roll-Out entstehenden Leitfaden zum Einsatz von MS 365 und AHP – Veröffentlichung wird im Intranet erfolgen
- die Datenschutzfolgeabschätzung – Veröffentlichung wird im Intranet erfolgen
- MS Teams ist eine sich laufend fortentwickelnde Anwendung. Dem entsprechend wird eine sequenzielle Anpassung dieser Anlage erfolgen.

Version 1, Stand 12.1.2022

Anlage 3

Vereinbarung über ergänzende Regelungen zur mobilen Nutzung von Microsoft 365- Anwendungen über mobile Endgeräte gemäß § 5 Abs. 4 DV Microsoft 365

1. Variante AHP-Arbeitsplatz

Über den AHP-Arbeitsplatz ist eine uneingeschränkte Nutzung möglich.

2. Variante klassischer Arbeitsplatz

Eine Nutzung ist außerhalb der Bereiche

Meldewesen

Personalverwaltung

Kindertagesstätten Verwaltung

möglich.

Version 1, Stand 12.1.2022

Anlage 4

Dokumentation sämtlicher Schnittstellen gemäß § 6 Abs. 2 DV Microsoft 365

Derzeit kein Fall zur Regelung.

Version 1, 12.01.2022

Anlage 5

Allgemeines Rollen- und Berechtigungskonzept

gemäß § 8 Abs. 2 DV Microsoft 365

1. Begriffsbestimmungen

R – Responsible:
Wer ist für die Durchführung der Aufgabe verantwortlich? Genannt wird üblicherweise eine Person, auch wenn diese weitere Personen zur Abarbeitung der Aufgabe hinzuziehen kann.

A – Accountable:
Wer entscheidet, ob die Aufgabe korrekt durchgeführt wurde? Oft delegiert diese Person eine Aufgabe an die „responsible“ Person und prüft die Ergebnisse der Durchführung.

C – Consulted:
Wer wird zur Durchführung der Aufgabe befragt? Hier handelt es sich oft um Fachexperten oder Dritte, die nicht direkt an der Durchführung beteiligt sind, die jedoch beratend zur Seite stehen.

I – Information

2. Variante AHP-Arbeitsplatz

		Verantwortliche							
		Microsoft (durch ADV-Vereinbarung zu verpflichten)	Cancom (durch ADV-Vereinbarung zu verpflichten)	LKA, Bereich ELKB-IT	LKA Abteilungen	IT-Multiplikatoren	andere Verwaltungs-einrichtungen	Nutzende verantwortliche Stellen (KG, DB-u.a. im Sinne der verfassten Kirche)	Einzel-nutzer
Durchführung der DSFA und deren Fortentwicklung				R	A	C	A	A	
Abschluss der ADV-Verträge sowie wesentliche Inhalte				R		C	A	A	
Technische Datenschutzmaßnahmen, § 27 DSG-EKD	Die verantwortliche Stelle (i.d.R. der Vertragspartner von Microsoft/ Cancom) ist verantwortlich für die Umsetzung der Technischen Maßnahmen	R	R	A	I	C	C, I	C, I	
Organisatorische Datenschutzmaßnahmen, § 27 DSG-EKD	Die verantwortliche Stelle (i.d.R. der Vertragspartner von Microsoft/ Cancom) ist verantwortlich für die Umsetzung der Organisatorischen Maßnahmen	R	R	A, R	A	C	A, C, I	A, C, I	
Privacy by Design & Default, § 28 DSG-EKD	Datenschutz durch Technikgestaltung, Datenschutzfreundliche Voreinstellungen (Default),	R	R	A	A	C	C, I	C, I	
Informationspflichten, Auskunft, §§ 17-19 DSG-EKD	die verantwortliche Stelle gibt Auskunft			I	R	C	R	R	
Gewährung von Rechten gem. §§ 20-25 DSG-EKD	die verantwortliche Stelle gibt Auskunft			R	R	C	R	R	
Pflege des VvV, § 31 DSG-EKD	Verzeichnis von Verarbeitungstätigkeiten			R	A	C	A	A	
Meldung von Datenpannen, §§ 32,33 DSG-EKD	Nutzer müssen zur Meldung einer Datenpanne geschult werden	R	R	R	R	R	R	R	R
Sorgfaltspflichten aus Arbeitsverhältnis	**Umgang mit IT und Daten**				A	C	A	A	R

3. Variante klassischer Arbeitsplatz

			Verantwortliche				
			Microsoft (durch ADV-Vereinbarung zu verpflichten)	Cancom (durch ADV-Vereinbarung zu verpflichten)	LKA, Bereich ELKB-IT	ggf. IT-Multiplikatoren	Dienststelle und Einzel-nutzer
Befugnisse und Verantwortlichkeiten	Durchführung der DSFA und deren Fortentwicklung				R	C	
	Abschluss der ADV-Verträge sowie wesentliche Inhalte				R	C	
	Technische Datenschutzmaßnahmen, § 27 DSG-EKD	Die verantwortliche Stelle (i.d.R. der Vertragspartner von Microsoft/ Cancom) ist verantwortlich für die Umsetzung der Technischen Maßnahmen	R	R	A	C	R, A, C ,I
	Organisatorische Datenschutzmaßnahmen, § 27 DSG-EKD	Die verantwortliche Stelle (i.d.R. der Vertragspartner von Microsoft/ Cancom) ist verantwortlich für die Umsetzung der Organisatorischen Maßnahmen	R	R	A, R	C	R, A, C ,I
	Privacy by Design & Default, § 28 DSG-EKD	Datenschutz durch Technikgestaltung, Datenschutzfreundliche Voreinstellungen (Default),	R	R	A	C	R, A, C ,I
	Informationspflichten, Auskunft, §§ 17-19 DSG-EKD	die verantwortliche Stelle gibt Auskunft			I	C	R, A, C ,I
	Gewährung von Rechten gem. §§ 20-25 DSG-EKD	die verantwortliche Stelle gibt Auskunft			R	C	R, A, C ,I
	Pflege des VvV, § 31 DSG-EKD	Verzeichnis von Verarbeitungstätigkeiten			R	C	R, A, C ,I
	Meldung von Datenpannen, §§ 32,33 DSG-EKD	Nutzer müssen zur Meldung einer Datenpanne geschult werden	R	R	R	R	R, A, C ,I
	Sorgfaltspflichten aus Arbeitsverhältnis	Umgang mit IT und Daten				C	R, A, C ,I

4. Rollen- und Berechtigungskonzept

- vgl. Anhang 4a) Steuerung Exchange-Online
- vgl. Anhang 4b) Steuerung von MS Teams

5. Hinweise

- Die Vergabe von Berechtigungen ist im Leitfaden beschrieben. Dieser wird laufend fortgeschrieben und im Intranet veröffentlicht werden.
- Der Gesamtausschuss erhält bezogen auf die Anhänge 4a) und 4b) jeweils die Rolle „Complianceverwaltung“

Version 1, Stand: 12.1.2022

Anlage 5 Anhang 4a)

Rollenbeschreibung	Name der Rolle	Art der Rolle	Rechte	Erläuterung
Es wird ermöglicht E-Mail-Adressen anzulegen und wieder zu entziehen; dem User werden die Zugangsdaten zur Implementierung gesendet	User-Anlage	technische Rolle	bestimmte Adminstratorenrechte	es muss die Möglichkeit bestehen zu prüfen, ob die E-Mail-Adresse angelegt wurde; es muss sichergestellt werden dass diese Rechte entzogen werden können ; Rechte sind auf diesen Bereich beschränkt ausgeführt über Cancom
Für einen User soll eine E-Mail-Adresse eingerichtet werden	E-Mail-Bereitstellung	organisatorische Rolle	Kompetenz/Autorität	über ein definierten Prozess werden einzurichtende E-Mail-Adressen zur Verfügung gestellt; über einen definierten Prozess werden E-Mail Adressen wieder entzogen (über BSZ zur Beauftragung an Cancom)
Mitglieder können in Übereinstimmung mit ihren Richtlinien Compliance-Einstellungen in Exchange konfigurieren und verwalten.	Complianceverwaltung	technische Rolle	Compliance-Administrator Dynamische Verteilergruppen Verhinderung von Datenverlust Verwaltung von Informationsrechten Journaling Nachrichtenverfolgung Aufbewahrungsverwaltung Transportregeln Überwachungsprotokolle nur anzeigen Schreibgeschützte Konfiguration Schreibgeschützte Empfänger Sicherheitsmonitoring	Für IT-Sicherheit und Datenschutzbeauftragte, um die Umgebung prüfen zu können. Zugriff auch für Gesamtausschuss
Mitglieder können die Konfiguration für einzelne Empfänger anzeigen und verwalten und Empfänger in einer Exchange-Organisation anzeigen. Mitglieder dieser Rollengruppe können nur die Konfiguration verwalten, die jeder Benutzer in seinem eigenen Postfach verwalten kann.	Helpdesk	technische Rolle	Kennwort zurücksetzen Benutzeroptionen Schreibgeschützte Empfänger etc. ohne zentrale Rechte	Benötigt für Benutzer Helpdesk der Firma Cancom bzw. örtliche IT-Verantwortliche und IT-Multiplikatoren Kommunikationsschnittstelle zu Cancom
Mitglieder haben administrativen Zugriff auf die gesamte Exchange Online Organisation und können fast jede Aufgabe in Exchange Online ausführen.	Organisationsverwaltung	technische Rolle	E-Mail-Richtlinien, E-Mail-aktivierte Öffentliche Ordner, Erstellen von E-Mail-Empfängern Mail-Tipps, Postfächer verschieben, Öffentliche Ordner, Empfängerrichtlinien, Aufbewahrungsverwaltung Benutzerdefinierte Apps einer Organisation, Marketplace-Apps einer Organisations Client Zugriff, Organisationskonfiguration, Organisations Transport Einstellungen Remote- und akzeptierte Domänen Rollenverwaltung, Sicherheitsadministrator, Erstellen und Mitgliedschaft von Sicherheitsgruppen, Sicherheitsleseberechtigter Team Postfächer, UM-Postfächer Transportregeln, Benutzeroptionen Verbundfreigabe Verwaltung von Informationsrechten, Journaling, Rechtliche Aufbewahrungspflicht	Mitarbeiter der Firma Cancom übernehmen die Administration und Konfiguration der Exchange Online Plattform

Zugriff auf die gesamte MS Cloud Umgebung	Globaler Administrator	technische Rolle	Sämtliche Rechte auf den gesamten MS Tenant	Adminteam Fa. Cancom, Notfalladmin Zugänge sind mit 2FA abgesichert und von den Konten, die für die tägliche Arbeit benutzt werden getrennt. Da nur ein anderer globaler Administrator das Kennwort eines globalen Administrators zurücksetzen kann, empfiehlt es sich, mindestens zwei globale Administratoren vorzusehen für den Fall, dass es zu einer Kontosperre kommt. Ein globaler Administrator hat jedoch fast unbegrenzten Zugriff auf die Einstellungen der Organisation und die meisten Daten.
Exchange Online umfasst eine Standard-Rollenzuweisungsrichtlinie. Benutzer, deren Postfächer dieser Rollenzuweisungsrichtlinie zugeordnet sind, können folgende Aufgaben ausführen:	Standard E-Mail Benutzerrechte	technische Rolle	Beitreten zu oder Verlassen von Verteilergruppen, die Mitgliedern das Verwalten der eigenen Mitgliedschaft gestatten. Anzeigen und Ändern grundlegender Postfacheinstellungen ihrer eigenen Postfächer. Dazu zählen z. B. Einstellungen für Posteingangsregeln, Rechtschreibprüfung, Junk-E-Mail und Microsoft ActiveSync-Geräte. Ändern ihrer Kontaktinformationen, z. B. geschäftliche Adresse und Telefonnummer, Mobiltelefonnummer und Pagernummer. Erstellen, Ändern oder Anzeigen von Einstellungen für Textnachrichten. Anzeigen oder Ändern von Voicemaileinstellungen. Anzeigen und Ändern ihrer Marketplace-Apps. Erstellen von Teampostfächern und Verbinden dieser Postfächer mit Microsoft SharePoint-Listen. Erstellen, Ändern oder Anzeigen von Abonnementeinstellungen für E-Mails, wie z. B. Nachrichtenformat und Protokollstandards.	Anwenderinnen und Anwender benötigen diese Berechtigungen um Ihr E-Mail Postfach und Ihre Kontakte zu verwalten
Administrative Berechtigung auf Benutzerkontenebene	Benutzeradministrator	technische Rolle	Benutzer und Gruppen hinzufügen Lizenzen zuweisen Die meisten Benutzereigenschaften verwalten Benutzeransichten erstellen und verwalten Kennwortablaufrichtlinien aktualisieren Serviceanfragen verwalten Den Dienststatus überwachen Benutzernamen verwalten Benutzerkonten löschen und wiederherstellen Kennwörter zurücksetzen Die Abmeldung von Benutzern erzwingen (FIDO)-Geräteschlüssel aktualisieren	Benutzer Helpdesk Fa. Cancom und Mitarbeiter im BSZ LKA, örtliche IT-Verantwortliche und IT-Multiplikatoren
Kann Benutzern Lizenzen zuweisen, diese entfernen und deren Verwendungsstandort bearbeiten	Lizenzadministrator	technische Rolle	Lizenzen zuweisen und entziehen	Die Firma Cancom weist den E-Mail Konten die erforderlichen Lizenzen zu bzw. entzieht diese wieder. (Exchange Online, ATP, Backup, etc.) Anforderung über Benutzer selbst direkt an Cancom

Rollenbeschreibung	Name der Rolle	Art der Rolle	Rechte	Erläuterung
Anlage eines Teambesitzer; Teambesitzer verwalten bestimmte Einstellungen für das Team. Sie können Mitglieder hinzufügen und entfernen, Gäste hinzufügen, Teameinstellungen ändern und Verwaltungs-To-dos erledigen. Ein Team kann mehrere Besitzer haben. siehe Leitfaden Mobile Arbeitsplätze	Teambesitzer-Anlage	technische Rolle	bestimmte Adminstratorenrechte	Es muss sichergestellt werden dass diese Rechte entzogen werden können ; Rechte sind auf diesen Bereich beschränkt, der Administrator muss (im Vier-Augen-Prinzip) auch Teams und deren Inhalte in Sharepoint löschen können Vergabe über Cancom Anforderung über Geschäftsführung der organisatorischen Einheit
Für definierte User-Gruppen werden Teambesitzer-Rechte vergeben.	Rollenberechtigung zuweisen	organisatorische Rolle	Kompetenz/Autorität	über einen definierten Prozess werden Teambesitzer-Berechtigungen vergeben und können wieder entzogen werden (über den technischen Admin) - wird nur über Cancom ausgeführt
Teams löschen; nicht mehr genutzte Teams müssen nach Prüfung gelöscht werden; Aufnahme in Leitfaden	Administrator Rollen-und Berechtigungen	technische Rolle	bestimmte Administratorenrechte Hinweis: jeder Bürger kann Klagen gegen immatriellen Verletzung seiner Persönlichkeitsrechte	Diese unterstützt u.a. die Datenminimierung und allgemein das Datenmanagement; die Löschung eines Teams sollte immer im Vier-Augen-Prinzip erfolgen bspw. Freigabe durch Organsisation, dann technische Löschung); Prozess sollte pragmatisch als möglich sein ggf. in jedem Quartal die Aktivitäten der Teams prüfen; User sollte über einen solchen Prozess infomriert sein. Anforderung über Entscheidungsinstanz auf Verbundebene Prüfung über ELKB-IT bzw. Compliance Team Beauftragung zur Umsetzung an Cancom durch ELKB-IT
Teambesitzer haben weitgehende Rechte in Teams u.a. Teams erstellen, Teamnamen bearbeiten; ausgesuchte Anwendungen hinzufügen; Teams löschen; Für die einnhame der Rolle benötuigt es einen durch die Organsiation definierten Rahmen (Compliance), der durch die Organisation bestimmt wird	Compliance-Team	organisatorische Rolle	Vorgaben zur Erstellung eines Teams; zur Einladung von Gästen; allgemeine Verhaltensempfehlungen; Vorgaben zum Austausch von Daten etc.	Das Compliance-Team definiert die Voraussetzungen zur Vergabe der Teambesitzer-Rolle; Nomenklatur zur Anlage von Teams; Rahmenbedingungen für eine Löschung eines Teams; Rahmenbedingunge für die Einladung von Gästen etc. Vorgaben müssen ausreichend flexibel sein und zeitgleich Anforderungen an Datenminmierung, Transparenz, Intervernierbarkeit gerecht werden aktuell Projektteam später ELKB-IT (Referat I.5) + ISB + DSB + GA
Mitglieder können Exchange-Antispamfunktionen verwalten, Berechtigungen für Antivirus-Produkte zur Integration mit Exchange erteilen und Nachrichtenfluss Regeln verwalten.	Nachrichtenschutz	technische Rolle	Transport Hygiene Schreibgeschützte Konfiguration Schreibgeschützte Empfänger	Zur Zeit nicht verwendet
Administration der Sharepoint und/ oder OneDrive-Umgebung (insbesonder Sharing)	Adminstrator Rollen- und Berechtigungen	SharePoint-Administrator	vergibt Freigabeeinstellungen zum Austausch von Daten via SharePoint; es gibt u.a. die Möglichkeit bestimmte Sicherheitsgrupen anzulegen und dort ggf. externe Freigaben zu verwalten; Gästen nur eine eingeschränkte sharin-Funktion ermöglichzen etc. ; diese Rechte müssen im SharePoint Admin Center vergeben werden	Dies erfolgt durch den technischen Admin unter Einbezug des Compliance Teams/ Projektteam
Einführung in die Nutzung in Teams	User-Unterstützung	organisatorische Rolle	Ist erster Ansprechpartner bei Fragen zur Erstellung eines Teams;	Untzersützt die Orgnaisationen vor Ort bei der Einführung von teams unter Berücksichtigung der Compliance Anforderungen IT-Multiplikator erkärt perspektiv die Nutzung und Strukturen von MS Teams
Zugriff auf die gesamte MS Cloud Umgebung	Globaler Administrator	technische Rolle	Sämtliche Rechte auf den gesamten MS Tenant	Adminteam Fa. Cancom, Notfalladmin Zugänge sind mit 2FA abgesichert und von den Konten, die für die tägliche Arbeit benutzt werden getrennt. Da nur ein anderer globaler Administrator das Kennwort eines globalen Administrators zurücksetzen kann, empfiehlt es sich, mindestens zwei globale Administratoren vorzusehen für den Fall, dass es zu einer Kontosperre kommt. Ein globaler Administrator hat jedoch fast unbegrenzten Zugriff auf die Einstellungen der Organisation und die meisten Daten.