EVANGELISCHE KIRCHE
IN MITTELDEUTSCHLAND

Vereinbarung

- über die Nutzung von Privatgeräten zu betrieblichen Zwecken (BYOD) -

Erstellt durch:	LKA-ISB, Sicherheitsbeauftragter
Bearbeitet durch:	Henze, Annekathrin
Freigegeben durch:	Henze, Annekathrin
Klassifizierung:	Intern
Datum der Version:	10.12.2020 11:54:53 , Version 3.0

EVANGELISCHE KIRCHE
IN MITTELDEUTSCHLAND

Inhaltsverzeichnis

Vereinbarung

über die Nutzung von Privatgeräten zu betrieblichen Zwecken (BYOD)

1. *Änderungshistorie*

Änderungshistorie

Status	Geändert durch	Datum/Uhrzeit	Version	Beschreibung
Freigegeben	Henze, Annekathrin	10.12.2020 11:54:53	3.0	Das Dokument wurde freigegeben.
Freigabeprozess gestartet	LKA-ISB, Sicherheitsbeauftragter	10.12.2020 11:53:37	2.1	Der Freigabeprozess wurde gestartet.
Geändert	LKA-ISB, Sicherheitsbeauftragter	10.12.2020 11:52:57	2.1	Korrekur
Nicht Freigegeben	Henze, Annekathrin	10.12.2020 11:49:59	2.0	Korrektur
Freigegeben	Henze, Annekathrin	09.12.2020 10:46:26	1.0	Das Dokument wurde freigegeben.
Freigabeprozess gestartet	LKA-ISB, Sicherheitsbeauftragter	09.12.2020 10:42:56	0.2	Der Freigabeprozess wurde gestartet.
Geändert	LKA-ISB, Sicherheitsbeauftragter	09.12.2020 10:42:13	0.2	Die Klassifizierung des Dokuments wurde geändert.
Erstellt	LKA-ISB, Sicherheitsbeauftragter	09.12.2020 10:41:46	0.1	Das Dokument wurde erstellt.

Vereinbarung zwischen den Parteien

Vorname: .....

Nachname: .....

Straße, Hausnr. : .....

PLZ, Ort, Land: .....

Optional:
Titel/ Position/ Mitarbeiternummer: .....

- nachfolgend bezeichnet als *„Mitarbeitende*“ –

trifft mit

Landeskirchenamt der EKM
Michaelisstraße 39
99084 Erfurt

- nachfolgend bezeichnet als *„Dienststelle*“ -

die folgende Vereinbarung über die Nutzung von Privatgeräten zu betrieblichen Zwecken und verpflichtet sich die vereinbarten Schutz-, Trennungs- und Informationspflichten zu beachten sowie Zutritts- und Kontrollrechte zu gewähren.

Präambel

Diese Vereinbarung über die Nutzung von Privatgeräten zu betrieblichen Zwecken ist verbindlich, wenn Sie private Geräte, wie z. B. mobile Telefone oder Computer für betriebliche Zwecke einsetzen. Die Vereinbarung gilt insbesondere, wenn auf den Geräten betriebliche Informationen, beispielsweise personenbezogene Daten oder Geschäftsgeheimnisse gespeichert werden oder Sie mittels der Geräte auf diese Informationen zugreifen (z. B. beim Zugriff auf die informationstechnische Infrastruktur der Dienststelle). Mit der Vereinbarung kommt die Dienststelle ihren gesetzlichen und vertraglichen Pflichten zum Schutz von betrieblichen Informationen und zur Belehrung der Mitarbeitenden nach.

Erläuterungen zu den verwendeten Begrifflichkeiten, insbesondere zum Begriff der betrieblichen Informationen, finden Sie auf dem Merkblatt im Anschluss an die Vereinbarung. Bei Fragen oder sonstigem Klärungsbedarf wenden Sie sich bitte an Ihre Vorgesetzten.

2. *Erlaubte Privatgeräte und erlaubte Software*

a. **Für die betriebliche Nutzung zugelassene Privatgeräte:** Für die betriebliche Nutzung sind ausschließlich private Geräte zugelassen, die in der Anlage zu dieser Vereinbarung genannt werden und die in dieser Vereinbarung genannten Voraussetzungen erfüllen. Die Verwendung anderer privaten Geräte für betriebliche Zwecke ist nicht erlaubt.

b. **Für die betriebliche Nutzung zugelassene Software:** Mitarbeitende dürfen bei der betrieblichen Nutzung von Privatgeräten nur die in der Anlage zu dieser Vereinbarung genannten oder durch die Dienststelle installierte Software nutzen. Die Nutzung anderer Software für betriebliche Zwecke ist nicht erlaubt.

c. **Aktualisierung der Anlage zumindest in Textform (z. B. E-Mail):** Bei Bedarf, z. B. beim Wechsel der Privatgeräte, muss die Anlage aktualisiert werden. Die Aktualisierung kann in Schriftform oder elektronisch in Textform erfolgen (z. B. per E-Mail). Die aktualisierte Anlage ist zusammen mit der Vereinbarung aufzubewahren.

d. **Besonders schützenswerte betriebliche Informationen:** Besonders schützenswerte betriebliche Informationen dürfen auf Privatgeräten, vorbehaltlich einer ausdrücklichen Erlaubnis, nicht verarbeitet werden.

e. **Gesonderte Freigabe für Nutzung im Home- und Mobile-Office:** Die Erlaubnis für eine betriebliche Nutzung von Privatgeräten umfasst nicht automatisch eine Erlaubnis zur Verrichtung von Arbeitstätigkeiten am Heimarbeitsplatz oder am mobilen Arbeitsplatz (so genanntes "Home-Office" und "Mobile-Office"). Wurde eine Erlaubnis für die Nutzung eines Heim- und/oder eines mobilen Arbeitsplatzes erteilt, gelten die von der Dienststelle erteilten Vorgaben zum Schutz von betrieblichen Arbeitsmitteln vor Zugriff durch unbefugte Personen auch für betrieblich genutzte Privatgeräte.

3. *Nutzungsumfang und Nutzungszeiten*

a. **Bereitstellung und Verfügbarkeit:** Sofern Privatgeräte nicht nur alternativ zu vorhandenen betrieblichen Arbeitsmitteln verwendet werden, sondern Voraussetzung für die Durchführung der Arbeitstätigkeit des bzw. der Mitarbeitenden ist, stellt der bzw. die Mitarbeitende deren Verfügbarkeit während der vereinbarten Arbeitszeiten und zu den vereinbarten Zwecken sicher.

b. **Beschränkung auf die Arbeitszeit:** Die Dienststelle weist darauf hin, dass Privatgeräte nur innerhalb der vereinbarten Arbeitszeit und etwaiger vereinbarter Überstunden oder Bereitschaft zu betrieblichen Zwecken eingesetzt werden und diese Arbeitszeiten nicht überschritten werden dürfen. Soweit nicht ausdrücklich anders vereinbart, führt die betriebliche Nutzung von Privatgeräten nicht zu einer Pflicht, für die Dienststelle fortwährend, auch außerhalb der Arbeitszeit, erreichbar sein zu müssen.

c. **Privatnutzung während der Arbeitszeit:** Während der Arbeitszeit gelten für die Privatnutzung der Privatgeräte dieselben Vorgaben wie für die private Nutzung betrieblicher Arbeitsmittel. Das bedeutet, dass die Privatnutzung während der Arbeitszeit grundsätzlich verboten ist und die Privatnutzung durch die Dienststelle erlaubt werden muss (dies gilt nicht, wenn die Privatnutzung erforderlich ist, z. B. in Notlagen).

4. *Trennungsgebot*

a. **Trennung zwischen privaten und betrieblichen Informationen:** Die betrieblichen Informationen (was auch Inhalte, wie z. B. Texte, Grafiken oder Videos umfasst) sind auf den Privatgeräten nach Möglichkeit der zur Verfügung stehenden Optionen, von den privaten Informationen zu trennen (z. B. durch unterschiedliche Arbeitsumgebungen oder Speicherung in getrennten Ordnern).

b. **Einrichtung betrieblicher Nutzerumgebung:** Sofern die betrieblich genutzten Privatgeräte oder die betrieblich genutzte Software dies erlauben, werden Mitarbeitende für betriebliche Zwecke eine eigene, sofern möglich zugangsgesicherte, Nutzerumgebung oder Zugänge einrichten (z. B. unterschiedliche Benutzerumgebungen auf Computergeräten).

c. **Betriebliches Gerätemanagement:** Die Dienststelle ist berechtigt, unter Mitwirkung des bzw. der Mitarbeitenden auf den Privatgeräten eine eigene Nutzerumgebung oder Softwareumgebung (zusammen als „Geräteumgebung“ bezeichnet) einrichten sowie entfernen zu können (z. B. so genannte „Container-Lösungen“). Die betriebliche Nutzung ist in diesem Fall, auf die in dieser Geräteumgebung installierte Software und gespeicherte Daten zu begrenzen. Diese Geräteumgebung darf nicht für private Zwecke genutzt werden.

d. **Speicherung von betrieblichen Informationen auf Privatgeräten:** Eine Speicherung von betrieblichen Informationen auf dem Privatgerät darf nur im Rahmen der für die betriebliche Nutzung freigegebenen oder installierten Software oder sonst mit Zustimmung der Dienststelle erfolgen. Dasselbe gilt für die Speicherung von Zugangsinformationen zu informationstechnischen Systemen der Dienststelle.

e. **Externe Speicherung betrieblicher Informationen und Nutzung privater Cloud-Dienste:** Eine Speicherung von betrieblichen Informationen außerhalb der für die betriebliche Nutzung zugelassenen Privatgeräten und Software ist nicht erlaubt. Die Mitarbeitenden müssen insbesondere sicherstellen, dass keine automatischen Kopien der betrieblichen Informationen erstellt und in privaten Cloud-Speichern gesichert werden.

5. *Eigentum, Besitz und Entsorgung*

a. **Eigentum und Besitz:** Der bzw. die Mitarbeitende sichert zu, dass das betrieblich genutzte Privatgerät in seinem bzw. ihrem Privateigentum steht und verpflichtet sich, das Privatgerät nicht zu vermieten, es nicht zu verleihen oder sich sonst vorsätzlich oder fahrlässig seines Besitzes zu begeben. Ebenso untersagt ist es, das Privatgerät, z. B. durch Verpfändung, zu belasten.

b. **Durchführung von Reparaturen:** Sollen Privatgeräte repariert werden, stellt der bzw. die Mitarbeitende sicher, dass die Reparaturstelle keinen Zugang zu betrieblichen Informationen erhalten kann und löscht diese nach Rücksprache mit der Dienststelle grundsätzlich vorab.

c. **Entsorgung von Altgeräten:** Im Fall der Entsorgung als Altgerät müssen alle betrieblichen Informationen und Möglichkeiten zu diesem Zugang zu erhalten sowie zur betrieblichen Nutzung überlassene Software, von dem Privatgerät gelöscht werden. Vorgaben der Dienststelle für eine sichere Löschung von Daten und Vernichtung von Altgeräten sind zu beachten. Etwaige, durch die Vorgaben der Dienststelle verursachte Mehrkosten trägt die Dienststelle, wobei mit ihr vorab Rücksprache zu halten ist.

d. **Geltendmachung von Besitz- und Eigentumsansprüchen:** Der bzw. die Mitarbeitende berechtigt der Dienststelle, Besitz- oder Eigentumsansprüche des bzw. der Mitarbeitenden geltend zu machen und gerichtlich durchzusetzen. Voraussetzung ist, dass die Geltendmachung und Durchsetzung der Ansprüche erforderlich ist, um die Interessen der Dienststelle am Schutz der betrieblichen Informationen zu wahren und mildere Maßnahmen, z. B. eine Entfernung von Zugangsmöglichkeiten oder Fernlöschung von Daten nicht oder nicht mit demselben Grad der Sicherheit durchgeführt werden können.

6. *Allgemeine Verhaltens-, Schutz- und Informationspflichten*

a. **Schutz vor Zugriff durch unbefugte Personen:** Der bzw. die Mitarbeitende muss sicherstellen, dass unbefugte Personen keinen Zugang zu betrieblichen Informationen, die entweder auf dem Privatgerät gespeichert oder mittels des Privatgerätes zugänglich sind, erhalten. Insbesondere muss der bzw. die Mitarbeitende einen Zugriff durch unbefugte Personen auf die informationstechnische Infrastruktur der Dienststelle und auf Zugangsdaten (z. B. Logins und Passwörter) verhindern.

b. **Gewährung des Zugriffs auf Privatgeräte:** Es ist nicht erlaubt unbefugten Personen einen Zugriff auf die Privatgeräte zu gewähren (z. B. durch Überlassung des Passworts an Familienmitglieder). Sofern ein Zugang erforderlich sein sollte, darf er nur unter Aufsicht gewährt werden und nur wenn keine Offenbarung betrieblicher Informationen zu befürchten ist (z. B. ist die kurzfristige Nutzung eines Mobiltelefons durch ein Familienmitglied, dem die Nutzung betrieblicher Software und betrieblicher Informationen untersagt und Missbrauch nicht zu befürchten ist, erlaubt).

c. **Sperrung des Zugangs zu Privatgeräten:** Der bzw. die Mitarbeitende muss den Zugang zu den Privatgeräten sperren, wenn diese nicht genutzt werden. Die Sperrung setzt zumindest die Eingabe eines sicheren Passworts oder Nutzung biometrischer Zugangsdaten (z. B. Finger- oder Gesichtserkennung) voraus. Privatgeräte die betrieblich genutzt werden, dürfen nicht unbeaufsichtigt gelassen werden, wenn ein Zugang oder Wegnahme durch unbefugte Personen nicht ausgeschlossen werden kann. Wenn möglich, sind Privatgeräte in einem sicheren und gegen Wegnahme besonders geschützten Behältnis aufzubewahren.

d. **Beachtung allgemeiner Geheimhaltungs- und Vertraulichkeitspflichten:** Bei der betrieblichen Nutzung von Privatgeräten sind neben dieser Vereinbarung alle zwischen der Dienststelle und dem bzw. der Mitarbeitenden getroffenen Vereinbarungen, Verpflichtungen sowie erteilte Weisungen, insbesondere im Hinblick auf Vertraulichkeit, Verschwiegenheit und den Schutz von betrieblichen Informationen, zu beachten.

e. **Informationspflichten bei Gefährdung und Verletzung betrieblicher Informationen:** Der bzw. die Mitarbeitende wird die Dienststelle über mögliche stattgefundene oder drohende Verletzungen des Schutzes von betrieblichen Informationen, die zu seiner bzw. ihrer Kenntnis gelangt sind, bereits bei Verdacht und bei Auffälligkeiten unverzüglich informieren (z. B. bei unerlaubten Zugriff durch unbefugte Personen oder oder wenn unübliche technische Vorgänge bzw. Verhaltensweisen von Soft- und Hardware beobachtet werden).

f. **Informationspflichten bei Verlust oder Beeinträchtigung der Privatgeräte:** Der bzw. die Mitarbeitende wird die Dienststelle unverzüglich informieren, wenn das betrieblich genutzte Privatgerät

- verloren, gestohlen oder beschlagnahmt wurde oder sonst abhandengekommen ist oder beschädigt oder zerstört wurde;

- gepfändet wurde oder einem Insolvenzvermögen zugehörig ist.

Dies gilt auch, wenn das Privatgerät nur dem Zugriff auf die informationstechnische Infrastruktur der Dienststelle dient oder ein Verlust nur vorübergehend ist.

g. **Beachtung von Sicherheitsmaßnahmen und Umgehungsverbot:** Sicherheitsmaßnahmen, -verfahren und Vorrichtungen (z. B. Virenscanner, Firewalls, Verschlüsselungsmechanismen oder Freigabeprozesse für die Installation neuer Software) sind zu beachten und dürfen nicht abgeschaltet, verändert oder umgangen werden.

h. **Rechtsfolgen bei Missachtung der Vereinbarung:** Der bzw. die Mitarbeitende wird darauf hingewiesen, dass die Verletzung der Pflichten aus dieser Vereinbarung zu Datenschutzverstößen oder zur Beeinträchtigung des Schutzes von Geschäftsgeheimnissen oder sonstigen Nachteilen führen und Unterlassungs-, Beseitigungs- und Schadensersatz- sowie Auskunftsansprüche auslösen als auch in schweren Fällen (z. B. bei vorsätzlichen Datenschutzverstößen) zu einer Geld- oder Freiheitsstrafe führen kann. Eine Verletzung der Schutzpflichten kann zugleich eine Verletzung von Pflichten aus dem Dienst-/Arbeitsverhältnis darstellen und beispielsweise zu Abmahnung oder fristloser Kündigung führen.

7. *Hardware-, Software-, Netzwerk- und Kommunikationssicherheit*

a. **Beachtung von Software- und Sicherheitsaktualisierungen:** Die Software auf den Privaten Geräten muss stets auf dem aktuellen Stand gehalten werden. Software- und Sicherheitshinweise der Dienststelle sowie der Softwareanbieter sind zu beachten und umzusetzen.

b. **Verbindung mit fremden Geräten oder Software:** Der bzw. die Mitarbeitende stellt sicher, dass über Schnittstellen der Privatgeräte (z. B. USB-Verbindung, Bluetooth, Schnittstellen zu Cloud-Diensten und anderen Geräten) kein Zugriff durch unbefugte Personen auf betriebliche Informationen genommen werden kann.

c. **Verbot von Jailbreaking und illegaler Software:** Der Einsatz von unautorisierter oder unizensierter Software auf betrieblich genutzten Privatgeräten ist unzulässig (z. B. sog „Jailbreaking“ oder Nutzung sog. „Raubkopien“).

d. **Installation neuer Hardware und Software:** Der bzw. die Mitarbeitende darf keine Software oder Hardware auf den Privatgeräten installieren, die den Bestimmungen dieser Vereinbarung entgegensteht. Der bzw. die Mitarbeitende stellt vor der Installation sicher, dass neue Software oder Hardware den Schutz betrieblicher Informationen und die Einhaltung der Vorgaben dieser Vereinbarung nicht gefährdet. In Zweifelsfällen hält Der bzw. die Mitarbeitende Rücksprache mit der Dienststelle.

8. *Nutzung von Privatgeräten auf Reisen*

a. **Besondere Schutzmaßnahmen in Drittländern:** Werden Privatgeräte in Drittländer (d. h. Länder außerhalb der EU/EWR, bzw. der Schweiz) mitgenommen, so müssen entweder betriebliche Informationen und die Möglichkeiten des Zugriffs auf externe betriebliche Informationen vom Privatgerät gelöscht werden, außer die Mitnahme wurde durch die Dienststelle erlaubt.

b. **Ausloggpflicht bei Grenz- und Sicherheitskontrollen:** Werden auf Reisen außerhalb der EU/EWR und der Schweiz Grenzkontrollen und ausländische Sicherheitskontrollen passiert (z. B. auf Flughäfen), ist der bzw. die Mitarbeitende verpflichtet nicht nur den Zugang zum betrieblich genutzten Privatgerät zu sperren, sondern sich auch innerhalb der betrieblich verwendeten Software auszuloggen.

9. *Urheber- und Nutzungsrechte*

a. **Sicherstellung von Nutzungsrechten durch den bzw. die Mitarbeitende:** Der bzw. die Mitarbeitende stellt sicher, dass er bzw. sie über die nötigen Nutzungsrechte an der für betrieblichen Zwecke eingesetzten privaten Software verfügt. Insbesondere ist zu prüfen, ob eine kommerzielle, bzw. geschäftliche Nutzung zulässig ist. Sollten durch die betriebliche Nutzung der Software Kosten entstehen, die von der Dienststelle zu tragen sind, muss die Dienststelle diese Kosten vorab freigeben.

b. **Sicherstellung von Nutzungsrechten und Kostentragung durch die Dienststelle:** Die Dienststelle stellt sicher, dass sie über die nötigen Nutzungsrechte an der durch sie auf den Privatgeräten der Mitarbeitenden installierten oder zur Installation vorgegebenen Software verfügt und trägt die mit der betrieblichen Nutzung dieser Software verbundenen Kosten.

c. **Informationspflichten bei Geltendmachung von Schutzrechten durch Dritte:** Der bzw. die Mitarbeitende wird die Dienststelle unverzüglich informieren, wenn Dritte gegenüber dem bzw. der Mitarbeitenden Ansprüche aus der Verletzung von Schutzrechten wegen der von dem bzw. der Mitarbeitenden für die Dienststelle genutzten Software geltend machen.

d. **Haftung des bzw. der Mitarbeitenden:** Der bzw. die Mitarbeitende haftet für alle privat veranlassten Pflichtverletzungen, die unter Verwendung des Privatgeräts begangen werden, als auch dafür, dass das Privatgerät und etwaige Software für betriebliche Zwecke eingesetzt werden darf. Die Dienststelle ist nicht zur Prüfung der Berechtigung des bzw. der Mitarbeitenden zur Nutzung der Privatgeräte und privater Software zu betrieblichen Zwecken verpflichtet.

10. *Kontroll- und Zugriffsrechte*

a. **Kontrolle und Zugriff auf Privatgeräte:** Der bzw. die Mitarbeitende willigt ein, der Dienststelle die Erlaubnis der Kontrolle, des (Fern-)Zugriffs und der Einsichtnahme auf das betrieblich genutzte Privatgerät, sofern dies für die Dienststelle aufgrund zwingender gesetzlicher Pflichten oder sonst aufgrund berechtigter Interessen der Dienststelle erforderlich ist (z. B. aufgrund einer möglichen Verletzung des Datenschutzes oder einer angemessenen Überprüfung der Einhaltung dieser Vereinbarung) zu gewähren.

b. **Sicherstellung der Kontroll- und Zugriffsrechte als Bedingung:** Der bzw. die Mitarbeitende muss sicherstellen und im angemessenen Umfang nachweisen können, dass die Dienststelle die Kontroll- und Zugriffsrechte wahrnehmen kann. Ansonsten entfällt automatisch die Berechtigung des bzw. der Mitarbeitenden zur betrieblichen Nutzung des Privatgerätes, bei dem die Möglichkeit der Kontrolle und des Zugriffs nicht gewährleistet ist.

c. **Keine Leistungs- und Verhaltenskontrolle:** Mittels der betrieblich genutzten Privatgeräte findet bei deren privater Nutzung keine Leistungs- und Verhaltenskontrolle der Mitarbeitenden statt. Durch einen Zugriff auf private Informationen oder Software erlangte Informationen dürfen, bis auf Fälle eines betrieblichen Bezugs und schwerwiegender Pflichtverstöße oder Straftaten und auch dann nur im angemessenen und legalen Rahmen, nicht zur Kontrolle oder sonst zu Lasten des bzw. der Mitarbeitenden verwendet werden.

d. **Ortungs- und Sperrfunktionen für den Fall des Verlusts:** Die bzw. die Mitarbeitende erklärt sich mit der Installation von Software auf Privatgeräten einverstanden bzw. erlaubt der Dienststelle auf Funktionen Zugriff zu nehmen, die eine Ortung und/oder Sperrung der Privatgeräte für den Fall der Meldung des Verlusts oder ähnlicher Gefährdung betrieblicher Informationen durch den bzw. die Mitarbeitende erlaubt. Der Einsatz der Ortungs- und Sperrfunktionen muss für den Schutz betrieblicher Informationen erforderlich sein. Der Einsatz der Ortungs- und Sperrsoftware zu anderen Zwecken ist nicht erlaubt.

e. **Beschränkung auf betriebliche Informationen und Software:** Die Kontrolle, der Zugriff und die Einsichtnahme sind auf die betriebliche Software und betriebliche Informationen zu beschränken. Sofern die Dienststelle Zugriff auf private Informationen oder Software des bzw. der Mitarbeitenden erhält, hat sie den Zugriff sofort zu unterlassen und den bzw. die Mitarbeitende über den Zugriff zu informieren. Die Information darf nur dann unterbleiben, wenn sichergestellt ist, dass durch den Zugriff auf private Informationen keine Beeinträchtigung der Rechte und Interessen des bzw. der Mitarbeitenden zu befürchten ist.

f. **Verarbeitung von Mobilitätsdaten:** Die Dienststelle wird weder den Standort des bzw. der Mitarbeitenden noch seine bzw. ihre örtlichen Bewegungen mittels der Privatgeräte nachverfolgen oder sonst kontrollieren. Ausgenommen ist die Nutzung von Standort- und Bewegungsangaben, die gesondert vereinbart wurden oder Teil einer Softwarefunktion sind und dem bzw. der Mitarbeitenden bekannt sind und deren Einsatz für die betriebliche Nutzung der Privatgeräte im Einklang mit gesetzlichen Vorgaben erforderlich ist.

g. **Hinweis auf private Informationen:** Der bzw. die Mitarbeitende sorgt dafür, dass private Informationen vor einem zufälligen Zugriff durch die Dienststelle möglichst geschützt sind (z. B. durch Abgrenzung von betrieblichen Apps in gesonderten Ordnern oder Einrichtung von betrieblichen Arbeitsumgebungen) und weist die Dienststelle bei Gefahr eines unbeabsichtigten Zugriffs auf die privaten Informationen oder private Software hin.

h. **Protokollierung:** Die Kontrollmaßnahmen sind durch die Dienststelle zu protokollieren. Das Protokoll ist auf Verlangen dem bzw. der Mitarbeitenden Kopie zu überlassen.

11. *Vergütung und Kosten*

a. **Vergütung ist mit Arbeits- bzw. Mitarbeitervergütung abgegolten:** Mit der Vergütung des bzw. der Mitarbeitenden aus dem Dienst- und Arbeitsverhältnis ist auch die betriebliche Nutzung der Privatgeräte abgegolten. Eine zusätzliche Vergütung wird, unbeschadet gesetzlicher Vergütungspflichten, nicht geschuldet.

b. **Anschaffungs- und Betriebskosten:** Der bzw. die Mitarbeitende trägt alle in Zusammenhang mit der Anschaffung und dem Betrieb des Privatgerätes sowie Zubehör anfallenden Kosten.

c. **Verbindungskosten:** Der bzw. die Mitarbeitende trägt alle ihm bzw. ihr in Zusammenhang mit dem Betrieb des Privatgeräts entstehenden Verbindungskosten.

d. **Verlust, Beschädigung oder Zerstörung von Privatgeräten:** Die Dienststelle haftet anteilig für Verlust, Beschädigung oder Zerstörung der Privatgeräte sowie der privaten Software und privater Informationen, sofern diese durch eine betriebliche Nutzung ursächlich veranlasst waren, mit ihr adäquat zusammenhängen und insoweit der bzw. die Mitarbeitende kein Mitverschulden trägt. Im Übrigen werden die Kosten von dem bzw. der Mitarbeitenden getragen.

12. *Rechtsgrundlagen und Datenschutzhinweise*

a. **Rechtsgrundlage der Verarbeitung von Mitarbeiterdaten:** Die zur Durchführung dieser Vereinbarung und Verfolgung von Straftaten erforderliche Verarbeitung von personenbezogenen Daten der bzw. des Mitarbeitenden erfolgt auf Grundlage des § 49 Abs. 1, 2 DSG-EKD und sofern die Verarbeitung darüber hinaus zur Verfolgung von Pflichtverstößen erfolgt, auf Grundlage von § 6 Nr. 3, 4 und 8 DSG-EKD. Die Kontroll- und Zugriffsrechte nimmt die Dienststelle auf Grundlage einer Einwilligung gemäß § 6 Nr. 2 DSG-EKD und soweit besondere Kategorien von personenbezogenen Daten gemäß § 4 Nr. 2 DSG-EKD verarbeitet werden, zusätzlich auf Grundlage einer Einwilligung gemäß § 13 Abs. 2 Nr. 1 DSG-EKD wahr.

b. **Widerspruchsrecht:** Der bzw. die Mitarbeitende hat das Recht, aus Gründen, die sich aus seiner bzw. ihrer besonderen Situation ergeben, jederzeit gegen die Nutzung, bzw. die Verarbeitung seiner bzw. ihrer personenbezogenen Daten nach Maßgabe des Gesetzes Widerspruch einzulegen.

c. **Auskunfts- und weitere Rechte der Mitarbeitenden:** Der bzw. die Mitarbeitende kann nach Maßgabe des Gesetzes sein bzw. ihr Recht auf Auskunft oder Berichtigung, Löschung und Einschränkung der Verarbeitung ihrer personenbezogenen Daten sowie sein bzw. ihr Recht auf Übertragbarkeit von personenbezogenen Daten geltend machen und sich bei der zuständigen Aufsichtsbehörde beschweren. Der bzw. die Mitarbeitende kann die zuständige Aufsichtsbehörde bei der Dienststelle erfragen oder sich im Zweifelsfall an die am eigenen Wohnsitz oder am Sitz der Dienststelle zuständige Aufsichtsbehörde wenden.

13. *Laufzeit, Kündigung und Änderungen der Vereinbarung*

a. **Ordentliche Kündigungsfrist von zwei Wochen:** Diese Vereinbarung kann von dem bzw. der Mitarbeitenden und von der Dienststelle innerhalb einer angemessenen, die Interessen der beiden Vertragsparteien berücksichtigenden Frist, die im Regelfall zwei Wochen beträgt, ohne Begründung gekündigt werden.

b. **Außerordentliche Kündigung:** Eine außerordentliche Kündigung aus wichtigem Grund bleibt beiden Vertragsparteien vorbehalten. Ein wichtiger Grund liegt insbesondere vor, wenn die Trennungs- und Schutzpflichten entsprechend dieser Vereinbarung von dem bzw. der Mitarbeitenden schuldhaft missachtet werden und das Abwarten der ordentlichen Kündigungsfrist oder eine Ermahnung des bzw. der Mitarbeitenden der Dienststelle (z. B. wegen der Schwere der Verletzung oder sonstiger Zweifel an der Zuverlässigkeit des Schutzes betrieblicher Informationen) nicht zuzumuten ist.

c. **Fortbestehen der Pflichten nach der Vertragsende:** Die sich aus dieser Vereinbarung ergebenden Pflichten des bzw. der Mitarbeitenden gelten auch nach Ende der Vereinbarung im Hinblick auf die Berechtigungs-, Trennungs-, Schutz und Informationspflichten entsprechend dieser Vereinbarung fort, solange der bzw. die Mitarbeitende das Privatgerät zu betrieblichen Zwecken einsetzen sollte und/oder auf dem Privatgerät betrieblichen Informationen oder Zugangsmöglichkeiten zur informationstechnischen Infrastruktur der Dienststelle gespeichert hat.

d. **Form von Änderungen und der Kündigungserklärung:** Änderungen sowie Ergänzungen dieser Vereinbarung, als auch die Aufhebung dieser Formklausel und die Kündigung dieser Vereinbarung bedürfen der Schriftform oder eines durch die Dienststelle vorgesehenen adäquaten elektronischen Verfahrens.

14. *Löschung von betrieblichen Informationen*

a. **Rückgabe sowie Löschung von betrieblichen Informationen und Software:** Der bzw. die Mitarbeitende hat nach Beendigung dieser Vereinbarung oder jederzeit nach Aufforderung der Dienststelle, die auf dem Privatgerät befindlichen betrieblichen Informationen an die Dienststelle zurückzugeben und sie anschließend samt betrieblicher Software unverzüglich zu löschen oder die Übertragung und Löschung durch die Dienststelle zu dulden. Der bzw. die Mitarbeitende weist die Löschung der Dienststelle auf Anfordern im angemessenen Umfang, z. B. durch schriftliche Bestätigung oder die Möglichkeit einer Inaugenscheinnahme, nach.

b. **Entfernung von betrieblichen Informationen und Software durch die Dienststelle:** Die Dienststelle verpflichtet sich mit dem Ende dieser Vereinbarung, spätestens innerhalb von zwei Wochen, betriebliche Informationen, betriebliche Software und Zugänge von den Privatgeräten der Mitarbeitenden zu entfernen. Sofern zumutbar und die sichere Durchführung gewährleistet ist, kann die Dienststelle den bzw. die Mitarbeitende zur Durchführung der vorgenannten Maßnahmen auffordern. Die Dienststelle bestätigt dem bzw. der Mitarbeitenden auf Anfrage die Durchführung der Maßnahmen in Textform (oder falls von dem bzw. der Mitarbeitenden gefordert schriftlich) und erbringt bei begründeten Zweifeln erforderliche Nachweise. Die Einhaltung der vorgenannten Frist verlängert sich, sofern deren Verzögerung auf einer ausstehenden Mitwirkung des bzw. der Mitarbeitenden oder fehlendes Verschulden der Dienststelle beruht.

c. **Fernlöschung von betrieblichen Informationen und Software:** Die Dienststelle ist berechtigt die auf dem Privatgerät gespeicherten betrieblichen Informationen und betriebliche Software, sofern technisch möglich, aus der Ferne zu löschen. Der bzw. die Mitarbeitende erklärt sich mit der Installation entsprechender Software zu Zwecken der Fernlöschung einverstanden. Der bzw. die Mitarbeitende ist über eine Fernlöschung innerhalb angemessener Frist vorab, grundsätzlich drei Werktage, zu informieren (es sei denn der Vorabhinweis ist der Dienststelle, z. B. aufgrund einer unmittelbar drohenden Gefahr, nicht zuzumuten). Eine Fernlöschung ist erlaubt, wenn das Privatgerät beschädigt oder zerstört wird, gestohlen oder verloren gegangen ist, Anhaltspunkte für Missbrauch vorliegen (z. B. mehrfache Falscheingabe von Passwörtern) oder nach Beendigung dieser Vereinbarung.

d. **Keine Haftung für Löschung nicht getrennter privater Informationen:** Die Dienststelle haftet nicht für die Löschung etwaiger privater Informationen oder Software, die von dem bzw. der Mitarbeitenden nicht entsprechend dieser Vereinbarung von den betrieblichen Informationen getrennt wurden.

Ich habe eine Kopie dieser Vereinbarung sowie das Merkblatt mit Begriffserklärungen und Erläuterungen erhalten.

.....

Ort, Datum, Unterschrift des bzw. der Mitarbeitenden

.....

Ort, Datum, Unterschrift für die Dienststelle

Merkblatt mit Begriffserklärungen und Erläuterungen

a. **In diesem Merkblatt erhalten Sie Erklärungen und Erläuterungen zu den im Rahmen dieser Vereinbarung verwendeten Begrifflichkeiten:**
Betriebliche Informationen: Für die Zwecke dieser Vereinbarung sind „betriebliche Informationen" alle Informationen, die unabhängig von ihrer Bezeichnung ganz oder teilweise nicht für andere Unternehmen oder andere unbefugte Personen zugänglich sind und/oder Informationen, zu deren Schutz die Dienststelle verpflichtet ist. Zu den betrieblichen Informationen gehören insbesondere personenbezogene Daten und Geschäftsgeheimnisse, als auch betrieblich veranlasste Geschäftskontakte.

b. **Personenbezogene Daten:** „Personenbezogene Daten“ sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung (z. B. Cookie) oder zu einem oder mehreren besonderen Merkmalen, identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.

c. **Geschäftsgeheimnisse:** Als Geschäftsgeheimnisse im Sinne dieser Vereinbarung sind unabhängig von ihrer Bezeichnung (z. B. auch als Verwaltungs-, Betriebs- oder Fabrikationsgeheimnis) Informationen zu verstehen, die entweder ganz oder in Teilen unbefugten Personen, Unternehmen oder anderen Dritten nicht zugänglich sind und daher über einen wirtschaftlichen Wert für die Dienststelle verfügen. Ebenfalls als Geschäftsgeheimnisse sind Informationen zu verstehen, die gesetzlich als solche deklariert werden. Ein Geschäftsgeheimnis kann zudem dann vorliegen, wenn es durch den bzw. die Mitarbeitende im Rahmen seiner bzw. ihrer Arbeitstätigkeit geschaffen wurde, auch, wenn die Dienststelle von dem Geschäftsgeheimnis noch keine Kenntnis hat. Ein Geschäftsgeheimnis kann überdies die Information sein, dass die Dienststelle bestimmte Verfahren, Software oder Dienstleister einsetzt (auch, wenn diese selbst öffentlich bekannt sind). Zu den Geschäftsgeheimnissen können insbesondere Angaben zu Finanzvorgängen, Verwaltungsverfahren, Beratungsinhalten, Gemeindegliedern, Kunden, Mitarbeitenden, Ansprech- und Geschäftspartnern, zu Entwicklungs-, Planungs-, Herstellungs- und Vermarktungsverfahren, zu Software oder Knowhow der Dienststelle zählen.

d. **Besonders schützenswerte betriebliche Informationen und besondere Kategorien personenbezogener Daten:** Betriebliche Informationen sind besonders schützenswert, wenn der Zugang zu ihnen durch unbefugte Personen zu besonders hohen Schäden und schweren Nachteilen für die Dienststelle oder Dritte führen kann. Hierzu gehören z. B. Geschäftsgeheimnisse, deren Preisgabe die Tätigkeit der Dienststelle schwer gefährden oder erheblich belasten würde, Zugangsdaten (Logins, Passwörter, etc.) und besondere Kategorien personenbezogener Daten gemäß § 4 Nr. 2 DSG-EKD.

e. **Unbefugt:** Als unbefugt gelten Personen, Unternehmen oder sonstige Dritte, denen

die betrieblichen Informationen bestimmungsgemäß nicht zugänglich sind, insbesondere auch Familienmitglieder, Mitbewohner, Angehörige oder andere Mitarbeitende der Dienststelle gehören können.

f. **Zugang zu und Zugriff auf Informationen:** Unter Zugang zu und Zugriff auf Informationen ist die Möglichkeit zu verstehen, auf Informationen durch aktives Handeln (z. B. Aufruf von Dateien, Öffnen von Unterlagen) oder auch passive Offenbarung (z. B. Blick auf einen Bildschirm) zugreifen zu können.

Generell der Art nach zugelassene Privatgeräte:

- Mobiltelefone, Smartphones
- Desktop-Computer
- Tablets
- Mobile Computergeräte (Notebooks, Laptops)
- Druckgeräte
- Optische Scangeräte
- Foto- und Videokameras
- Mobile Festplatten
- USB-Flash-Speicher
- Optische Datenträger (CD, DVD, Blu-ray)
- Private Festnetztelefone
- Router und heimische Netzwerktechnologie

Anlage: Für die betriebliche Nutzung zugelassene Software

Die folgende Software darf für betriebliche Zwecke genutzt werden:

Beispiele:

- Office 365 (insbesondere Word, Excel, Powerpoint, Outlook) E- Mail-Software: Outlook von Microsoft in der jeweils aktuellen Version.

- Apps der Social-Media-Plattformen, nur wenn dienstlich notwendig (Facebook, Instagram, Twitter).

- Betriebsinterne Kommunikation (Microsoft Teams).

- Videokonferenzsysteme (Microsoft Teams, GoToMeeting, BBB etc., um als Gast an Videokonferenzen teilnehmen zu können)

- Webbrowser