

Durchführungsbestimmungen zur sicheren Nutzung mobiler und lokaler Endgeräte (DB-Endgeräte)

Vom 3. September 2024 (GVBl., Nr. 112, S. 207)

Der Evangelische Oberkirchenrat hat nach § 2 des Kirchlichen Gesetzes zur Ausführung des Kirchengesetzes über den Datenschutz der Evangelischen Kirche in Deutschland (AusG-DSG-EKD) vom 26. April 1994 (GVBl. S. 107), geändert am 23. Oktober 2013 (GVBl. S. 295) in Verbindung mit § 54 Abs. 2 des Kirchengesetzes über den Datenschutz der Evangelischen Kirche in Deutschland (DSG-EKD) vom 15. November 2017 (ABl. EKD S. 353), zuletzt geändert am 9. November 2022 (ABl. EKD S. 156) folgende Durchführungsbestimmungen erlassen:

§ 1

Geltungsbereich, Begriffsbestimmungen

- (1) ¹Diese Durchführungsbestimmungen finden Anwendung auf alle mobilen und lokalen Endgeräte, die auf das Cloudsystem von Microsoft 365 der Evangelischen Landeskirche in Baden zugreifen. ²Dieser Zugriff erfolgt für alle haupt- und ehrenamtlich tätigen Mitarbeitenden über eine persönliche E-Mail-Adresse mit der Endung @ekiba.de oder @*.ekiba.de.
- (2) Die Vorschriften des § 2 Abs. 1 Nummern 2 bis 5 finden keine Anwendung für vom Evangelischen Oberkirchenrat für seine Mitarbeitenden zur Verfügung gestellten mobilen und lokalen Endgeräte.
- (3) Mobile Endgeräte sind tragbare Kommunikationsgeräte, die ortsungebunden zur Sprach- und Datenkommunikation eingesetzt werden können, z. B. Mobiltelefone, Smartphones, Netbooks, Notebooks oder Tablets.
- (4) Lokale Endgeräte sind stationäre Geräte, die über einen Netzanschluss eines öffentlichen oder privaten Daten- oder Telekommunikationsnetzes angeschlossen sind, z.B. PCs.

§ 2

Nutzungsbedingungen

- (1) ¹Die in § 1 Abs. 1 Satz 1 genannten Endgeräte dürfen nur unter Beachtung der nachfolgend aufgeführten Bedingungen genutzt werden:
 1. Nutzerinnen und Nutzer sind verpflichtet, die von der Landeskirche vorgegebene Zwei-Faktor-Authentifizierung einzurichten und zu verwenden.

2. ¹Nutzerinnen und Nutzer sind für die Sicherung ihrer persönlichen Daten selbst verantwortlich. ²Der Evangelische Oberkirchenrat übernimmt im Falle einer aus Sicherheitsgründen erfolgten Rücksetzung keine Haftung für den Verlust von Daten.
 3. ¹Die Geräte sind mit den aktuellen Patches und Sicherheitsupdates des Herstellers oder Netzwerks auszustatten. ²Es ist mindestens einmal pro Woche zu überprüfen, ob neue Patches und Sicherheitsupdates vorhanden sind. ³Soweit vorhanden, sind diese unverzüglich zu installieren.
 4. ¹Alle installierten Anwendungen müssen Quellen (Google Play Store, Apple App Store) entstammen, die vom Entwickler des jeweiligen Betriebssystems autorisiert sind. ²Es darf kein Code von anderen Quellen installiert werden.
 5. Die Deaktivierung von werksseitig installierten Sperren mit dem Zweck, Zugriff auf eigentlich nicht für die Nutzerinnen und Nutzer vorgesehene Funktionen zu erhalten, ist nicht gestattet.
 6. Wird ein unbefugter Zugriff auf Daten der Landeskirche vermutet, ist dies dem Evangelischen Oberkirchenrat unverzüglich anzuzeigen.
 7. Raubkopien oder illegale Inhalte dürfen nicht auf Endgeräte geladen werden.
 8. Während der Nutzung von landeskirchlichen Anwendungen ist es den Nutzerinnen und Nutzern untersagt, auf einem mobilen oder lokalen Endgerät mit administrativen Benutzerrechten (Admin-Benutzer) zu arbeiten.
- (2) Die technischen Anforderungen nach § 3 bleiben unberührt.

§ 3

Technische Anforderungen

Die Nutzerinnen und Nutzer sind dafür verantwortlich, dass die Geräte folgende technische Voraussetzungen erfüllen:

1. Die in § 1 Abs. 1 Satz 1 genannten Geräte müssen ein aktuell gültiges Betriebssystem im Einsatz haben für das in regelmäßigen Abständen, mindestens alle 6 Monate, Sicherheitsupdates veröffentlicht werden.
2. Benutzerpasswörter für mobile und lokale Geräte dürfen nur in verschlüsselten Passwortspeichern aufbewahrt werden.
3. Benutzerpasswörter müssen den Anforderungen der Passworrichtlinie des Bundesamtes für Sicherheit in der Informationstechnik (BSI) genügen und dürfen nicht für andere Anwendungen verwendet werden.
4. Die Geräte müssen vor jeder erneuten Benutzung ein Passwort abfragen.

§ 4

Umfang der Serviceleistungen durch den Evangelischen Oberkirchenrat

- (1) Die Einrichtung und Konfiguration der Endgeräte erfolgt durch die Nutzerinnen und Nutzer selbst.
- (2) Für die Einrichtung der Zwei-Faktor-Authentifizierung stellt der Evangelische Oberkirchenrat Unterstützung in Form von Handreichungen bereit und unterstützt die Nutzerinnen und Nutzer im Rahmen des regulären IT-Supports.
- (3) „Für die Betriebssysteme iOS und Android stellt der Evangelische Oberkirchenrat eine Information zur Anbindung an das Mailsystem in der Infothek bereit.“ Weiterhin übernimmt die IT des Evangelischen Oberkirchenrats die Sicherstellung des Betriebs und der Verfügbarkeit des Mailsystems sowie den Support des Mailclients im Web.
- (4) Ein Support bei der Einrichtung und Konfiguration der Anbindung oder bei allgemeinen technischen Fragen, die das Endgerät betreffen, wird durch den Evangelischen Oberkirchenrat nicht geleistet.

§ 5

Inkrafttreten, Außerkrafttreten

- (1) Diese Durchführungsbestimmungen treten am 1. Oktober 2024 in Kraft.
- (2) Gleichzeitig treten die Durchführungsbestimmungen zur Datensicherheit mobiler und lokaler Endgeräte vom 20. Februar 2018 (GVBl. S. 166) außer Kraft.

