**Muster-Erklärung zur dienstlichen Nutzung privater Kommunikationsgeräte gemäß § 5 Abs. 4 IuK-Richtlinie**

Frau/Herr

|  |
| --- |
|  |

stellt unter Hinweis auf die anliegenden Nutzungsbedingungen sein privates Kommunikationsgerät für die dienstliche Nutzung für den Aufgabenbereich der

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

zur Verfügung.

Sie/Er versichert, die technisch-organisatorischen Maßnahmen zu treffen, die erforderlich sind, um den Belangen des Datenschutzes und der IT-Sicherheit Rechnung zu tragen.

|  |
| --- |
|  |

Ort, Datum

|  |
| --- |
|  |

Unterschrift

Anlage

Original zur Akte

Kopie an Mitarbeitende/n/Ehrenamtliche/n

**Nutzungsbedingungen bei der Nutzung privater Kommunikationsgeräte für den dienstlichen Gebrauch**

**Bring-Your-Own-Device (BOYD)**

Diese Nutzungsbedingungen sollen sicherstellen, dass beruflich oder ehrenamtlich Mitarbeitende, die eine Aufwandsentschädigung für die dienstliche Nutzung privater Kommunikationsgeräte erhalten, die Maßnahmen treffen, die erforderlich sind, um den Belangen des Datenschutzes und der IT-Sicherheit Rechnung zu tragen (vgl. § 5 Abs. 4 IuK-Richtlinie). Die entsprechenden Regelungen sind folgende:

IuK-Richtlinie, IT-Sicherheitsverordnung der EKD, Datenschutzgesetz der EKD.

Wenn Sie Daten verarbeiten, die unter das Seelsorgegeheimnis fallen, beachten Sie bitte das Seelsorgegeheimnisgesetz.

Die genannten Vorschriften können Sie digital abrufen unter

[www.kirchenrecht-evlka.de](http://www.kirchenrecht-evlka.de)

**Sicherheit - Generelle Hinweise**

* Die Endgeräte müssen sich in Ihrem dauerhaften Besitz befinden (keine Leihgeräte oder "Familiengeräte mit einem Account"), sodass Sie auch jederzeit dienstlichen Zugriff haben.
* Es sind Ihre Geräte, also sind Sie selbst verantwortlich für die Funktions- und Betriebsfähigkeit sowie die Einhaltung der Sicherheitsmaßnahmen (siehe Checkliste unten). Die Kirchenämter sind nur dafür verantwortlich, den Zugriff auf die kirchlichen IT-Dienste (Eintragung in das landeskirchliche Nutzer\*innenverzeichnis, Berechtigungsvergabe) einzurichten.
* Sollten Sie dienstlichen Daten auf Ihren Geräten erstellen oder bearbeiten, denken Sie bitte an eine Sicherung.
* Dritte, die nicht Mitarbeitende der Einrichtung sind, dürfen weder Zugang zu Ihrem PC noch zu Ihren dienstlichen Daten bekommen.
* Wenn Sie private Geräte nicht mehr für dienstliche Zwecke nutzen, z.B. weil Sie aus dem Dienst ausscheiden oder Ihr Ehrenamt aufgeben, dann sorgen Sie bitte auch dafür, dass sämtliche dienstlichen Daten von diesen Geräten entfernt werden.

**Maßnahmencheckliste (Minimum, nicht abschließend)**

* Dienstliche Daten müssen von privaten Daten getrennt werden. Legen Sie also z.B. einen Ordner mit der Markierung "privat" an und speichern Sie die Daten dort.
* Am besten richten Sie auf Ihrem Ihren PC ein spezielles Benutzerkonto mit eigenem Passwort (mind. 12 Zeichen) für die dienstlichen Aufgaben ein und speichern die dienstlichen Dokumente in diesem Profil. Nutzen Sie für private Dinge ein privates Benutzerkonto. Damit erreichen Sie eine gute Trennung.
* Sichern Sie Ihre dienstlichen Daten regelmäßig über die Kirchen-Cloud ([Seafile](https://sf.it.elkh.de/) oder intern-e), um diese vor Verlust durch Defekte zu schützen. Nutzen Sie Seafile oder intern-e auch sonst zum Speichern Ihrer dienstlichen Daten.
* Verschlüsseln Sie bei Notebooks Ihre Festplatte, z.B. bei Microsoft mit dem kostenlosen Tool Bitlocker, bei macOS mit FileVault. Damit vermeiden Sie, dass im Falle eines Geräteverlustes die Daten in unbefugte Hände geraten.
* Nutzen Sie die landeskirchlichen Dienste für dienstliche Aufgaben, z.B. ein dienstliches E-Mail-Postfach, Seafile und intern-e. Vermeiden Sie unbedingt private Accounts oder Dienste. Wenn Sie nicht genau wissen, was alles angeboten wird, fragen Sie in Ihrer Dienststelle nach.
* Zum Schutz vor Fremdzugriffen über das Netzwerk lassen Sie bitte die Betriebssystem-Firewall aktiviert.
* Verwenden Sie einen Virenscanner mit aktuellen Virensignaturen, z.B. bei Windows den Microsoft Defender.
* Halten Sie Ihr Betriebssystem immer auf dem aktuellen Stand, spielen Sie alle Sicherheitspatches, oder - wenn Sie wenig Erfahrung haben - einfach alle Updates, die Ihnen vom Betriebssystem angeboten werden, ein. Achten Sie auch insbesondere beim E-Mail-Programm und bei Ihrem Webbrowser stets auf Aktualität.

**Bring Your Own Support - IT-Support und Hilfe**

* Für den IT-Support sind Sie selbst verantwortlich.
* Falls es notwendig sein sollte, müssen Sie sich einen Dienstleister zur Unterstützung holen. Dieser darf keinen Zugang zu den dienstlichen Daten bekommen.
* Verwenden Sie keine Software aus unbekannten Quellen, z.B. unbekannte Websites. Auf der landeskirchlichen IT-Seite (<https://it.landeskirche-hannovers.de>) gibt es einen Katalog mit empfohlenen Programmen für den dienstlichen Arbeitsplatz. Im Download-Bereich (<https://it.landeskirche-hannovers.de/service/downlods>) können Sie sich auch speziell vorkonfigurierte Software herunterladen. Teilweise stellt Ihnen auch Ihre Dienststelle den Zugriff auf spezielle Fachanwendungen zur Verfügung, wenn es für Ihre Arbeit notwendig sein sollte. Fragen Sie bei Bedarf nach.
* In Notfällen (z.B.: Ihr Gerät geht verloren oder wird gehackt) wenden Sie sich auf jeden Fall umgehend an Ihre Dienststelle, um notwendige Maßnahmen abzustimmen. Bei Gefahr/Verdacht auf Missbrauch eines dienstlichen Kontos durch Unbefugte ändern Sie zusätzlich umgehend die Passwörter.
* Falls Sie die Passwörter nicht selbst ändern können, so wenden Sie sich an die IT Ihres zuständigen Kirchenamtes oder an die COMRAMO.
* Allgemeine Informationen zur Hilfe bei Problemen gibt es auf der landeskirchlichen IT-Seite (<https://it.landeskirche-hannovers.de>).

**Work-Life-Balance**

* Achten Sie bitte auch in Ihrer nicht dienstlichen Zeit darauf, dass der Zugriff auf dienstliche Daten durch Dritte nicht möglich ist.
* Auch wenn Sie jetzt immer und überall arbeiten können: Beenden Sie beim Feierabend den Zugriff auf dienstliche Daten, loggen sich aus dem PC/Account aus und verstauen Sie das Gerät unzugänglich für Dritte (und sich selbst) bis zum nächsten Tag.