Anlage:
Erläuterungen zu dem Muster für eine Dienstvereinbarung über die Nutzung privater Smartphones und Tablets für dienstliche Zwecke

1. **In § 1 Absatz 3 bedeutet „schriftlich“, dass die Anforderungen des §126 BGB an die Schriftform erfüllt sein müssen**:

   „(1) Ist durch Gesetz schriftliche Form vorgeschrieben, so muss die Urkunde von dem Aussteller eigenhändig durch Namensunterschrift oder mittels notariell beglaubigten Handzeichens unterzeichnet werden.
   (2) Bei einem Vertrag muss die Unterzeichnung der Parteien auf derselben Urkunde erfolgen. Werden über den Vertrag mehrere gleichlautende Urkunden aufgenommen, so genügt es, wenn jede Partei die für die andere Partei bestimmte Urkunde unterzeichnet.
   (3) Die schriftliche Form kann durch die elektronische Form ersetzt werden, wenn sich nicht aus dem Gesetz ein anderes ergibt.
   (4) Die schriftliche Form wird durch die notarielle Beurkundung ersetzt.“

   Bei „Textform“ in § 8 Absatz 1 und 5 müssen die Anforderungen in §126b BGB eingehalten werden:

   „Ist durch Gesetz Textform vorgeschrieben, so muss eine lesbare Erklärung, in der die Person des Erklärenden genannt ist, auf einem dauerhaften Datenträger abgegeben werden. Ein dauerhafter Datenträger ist jedes Medium, das

   1. es dem Empfänger ermöglicht, eine auf dem Datenträger befindliche, an ihn persönlich gerichtete Erklärung so aufzubewahren oder zu speichern, dass sie ihm während eines für ihren Zweck angemessenen Zeitraums zugänglich ist, und

   2. geeignet ist, die Erklärung unverändert wiederzugeben.“

2. Gemäß § 3 Absatz 2 des Musters für eine Dienstvereinbarung ist der Zugang zu dienstlichen Daten mit einem privaten Gerät nur über ein **Mobile-Device-Management-System** (nachfolgend: MDM) möglich. Daher werden im folgenden hierzu **Hinweise** gegeben:

   2.1 **Definition Mobile-Device-Management-System (MDM):** Dieses ermöglicht eine zentralisierte Administration, Kontrolle und Überwachung von Mobilgeräten wie Smartphones oder Tablets durch den Administrator mit Hilfe von Soft- und Hardware.
   Diese Geräte können unabhängig davon, ob sie von der Firma bereitgestellt oder im Eigentum der oder des Mitarbeitenden sind, angemeldet und konfiguriert werden. Die Geräte lassen sich mittels des MDM über eine Web-Konsole, bequem löschen oder sperren und deren Einstellungen können stets überwacht werden. Mittels spezieller Werkzeuge ist es je nach dem in der Einrichtung bereits vorhandenem System möglich, die Einhaltung unternehmenseigener Sicherheitsrichtlinien zu gewährleisten, Anwendungen/Apps zu verwalten, einen sicheren Zugang zum Firmennetzwerk zu garantieren und Verschlüsselungen vorzunehmen.

Anlage:
Erläuterungen zu dem Muster für eine Dienstvereinbarung über die Nutzung privater Smartphones und Tablets für dienstliche Zwecke

2.2 **Erläuterung der technischen Verfahren für MDM-Lösungen:** Für unabdingbare Trennung der Verwaltung und optimalerweise auch physischen Trennung des dienstlichen von dem privaten Bereich des Gerätes gibt es verschiedene technische Lösungen:

- Inventarisierung der Geräte und Verwaltung der Anwendungen/Apps
- Ausführen der dienstlichen Applikationen ausschließlich in einer isolierten virtuellen Umgebung (sog. „Sandboxing“)
- Micro-Virtualisierung: Verwaltung und Trennung der Bereiche über virtuelle Maschinen (VM-Ware) wie auch im Client-Server-Bereich.

Soweit in einer Einrichtung ein MDM noch ausgewählt werden kann, sind solche Systeme vorzuziehen, die eine klare und eindeutige technische Trennung/Abschottung der dienstlichen Umgebung und Anwendungen von dem privaten Bereich ermöglichen.

2.3 **Notwendigkeit der Klärung, welche Anwendungen auf dem Endgerät ausgeführt werden dürfen und welche explizit ausgeschlossen werden:** Es muss im Vorfeld explizit geklärt werden, welche Anwendungen bei der dienstlichen Nutzung des privaten Gerätes genutzt werden dürfen und welche nicht. Dies kann durch das MDM-System gesteuert werden. Für die Dokumentation und die Steuerung bietet sich hier das Instrument des Black- und/oder Whitelistings an, bei welchem die verbotenen und/oder erlaubten Anwendungen ausdrücklich aufgeführt werden.

3. **Bei der dienstlichen Nutzung der privaten Geräte ist keine Vermischung von dienstlichen und privaten Kalendern und Kontakten erlaubt:** Die Vermischung von dienstlichen und privaten Kalendern und Kontakten muss bei der dienstlichen Nutzung ausgeschlossen werden. Hier gibt es allerdings in den verschiedenen Landeskirchen, Werken und Einrichtungen zum Teil eine unterschiedliche Praxis und Gewohnheit. Es ist aber unbedingt erforderlich, für diese Frage eine juristische Klärung zu veranlassen.

4. **Notwendigkeit passender Lizenzen, Erläuterung zu § 4 Absatz 1:** Nicht jede Software ist zum beliebigen (privaten / kommerziellen) Einsatz vorgesehen. Viele Hersteller bieten unterschiedliche Lizenzmodelle für verschiedene Nutzungsarten an. So ist es beispielsweise denkbar, dass ein Softwarehersteller sein Produkt für den ausschließlich privaten Gebrauch deutlich günstiger oder sogar gratis anbietet. Die Teilnahme am BYOD-Programm kann es daher erforderlich werden lassen, andere Lizenzen zu beschaffen. Da dem Dienstgeber nicht bekannt ist, welche Software in welchem Lizenzmodell auf dem privaten IT-Gerät betrieben wird und es zudem eine Vielzahl von Lizenzmodellen gibt, kann eine solche Prüfung nur selbst durch die Teilnehmende oder den Teilnehmenden am BYOD-Programm erfolgen.

5. **Hinweis auf Vergütungs- und Steuerfragen:** Bei Kostenbeteiligung des Dienstgebers sind Fragen des Steuerrechts in Bezug auf eine Verpflichtung zur Versteuerung eines erlangten Vorteils zu prüfen.

6. **Dritte i. S. dieser Dienstvereinbarung** sind auch Ehepartner bzw. eingetragene Lebenspartner, Kinder und sonstige Familienangehörige.

Anlage:
Erläuterungen zu dem Muster für eine Dienstvereinbarung über die Nutzung privater Smartphones und Tablets für dienstliche Zwecke

7. **Die oder der Mitarbeitende darf nur dann an dienstlichen Daten arbeiten, solange sie oder er sich in einer vom Dienstgeber betriebenen, abgesicherten Netzinfrastruktur befindet:** Außerhalb dieser Netzwerkinfrastruktur ist das Arbeiten an und mit dienstlichen Daten und Anwendungen nur dann gestattet, wenn eine gesicherte Verbindung zur Netzwerkinfrastruktur des Dienstgebers aufgebaut worden ist (z.B. durch VPN-Tunnel) oder sämtliche Datenverbindungen des Endgerätes zuvor unterbrochen worden sind („Flugmodus“). Im Übrigen ist das Arbeiten an dienstlichen Daten untersagt.

8. **Verweise auf folgende Leitfäden mit Links:** Weitere ausführliche Informationen finden sich unter den folgenden Links:

   8.1 **Bundesamt für Sicherheit in der Informationstechnik:**

   https://www.bsi-fuer-buerger.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Download/Ueberblickspapier_BYOD_pdf.pdf

   8.2 **BITKOM:**

   https://www.bitkom.org/noindex/Publikationen/2013/Leitfaden/BYOD/130304-LF-BYOD.pdf

   8.3 **International Working Group on Data Protection in Telecommunications:**

   https://datenschutz-berlin.de/attachments/1083/675.49.11.pdf?1420541726

Hannover, den 12.05.2017