Dienstvereinbarung

über den Einsatz und die Nutzung von privaten und dienstlichen Endgeräten

(Smartphone und Tablet)

zwischen dem

Bistum Limburg

nachfolgend: „**Dienstgeber**“ genannt

- vertreten durch den Generalvikar -

und der

Hauptmitarbeitervertretung/Diözesane Arbeitsgemeinschaft der Mitarbeitervertretungen im Bistum Limburg (Haupt-MAV/DiAG)

nachfolgend: „**Haupt-MAV/DiAG**“ genannt

in der Fassung vom 01.05.2018

Inhaltsverzeichnis

A. Allgemeine Bestimmungen

§ 1 Geltungsbereich der Dienstvereinbarung

Diese Dienstvereinbarung gilt für alle Mitarbeiterinnen und Mitarbeiter des Bistums Limburg, des Domkapitels und der Kirchengemeinden (nachfolgend: „Beschäftigte").

§ 2 Begriffsbestimmungen

Der Dienstgeber und die Haupt-MAV/DiAG legen dieser Dienstvereinbarung die in **Anlage 1** geregelten Definitionen zu Grunde. Der Dienstgeber und die Haupt-MAV/DiAG werden, auch während des Bestehens dieser Dienstvereinbarung, auftretende Unklarheiten im Zusammenhang mit Begrifflichkeiten umgehend beseitigen und bei Bedarf die zu definierenden Begriffe der Anlage (auch zum Schutze der Beschäftigten) nachträglich hinzuzufügen. Änderungen oder Ergänzungen der Definitionen in Anlage 1 bedürfen der Einigung zwischen den Parteien, stellen aber keinen neuen Abschluss der Dienstvereinbarung dar.

§ 3 Gegenstand und Zielsetzung der Dienstvereinbarung

1. Der Dienstgeber möchte das flexible und mobile Arbeiten der Beschäftigten und besonders den mobilen Zugriff auf dienstliche Informationen über private Endgeräte fördern. Hierzu wird den Beschäftigten eine sog. MDM/MAM-Lösung bereitgestellt. Hierbei handelt es sich um eine Anwendung zum mobilen Gerätemanagement (Mobile Device Management, MDM) sowie für das Management mobiler Anwendungen (Mobile Application Management, MAM).
2. Die Dienstvereinbarung regelt die Rechte und Pflichten im Zusammenhang mit der Nutzung dieser MDM/MAM-Lösung auf

   a) privaten Endgeräten der Beschäftigten sowie
   b) bereitgestellten dienstlichen Endgeräten (nachfolgend: „Dienstgeräte").

§ 3 Anbieter

1. Die „MDM/MAM-Lösung" wird den Beschäftigten nach Vorlage der unterschriebenen Einwilligungserklärung Mobiles Arbeiten (Anlage 2) kostenfrei zur Verfügung gestellt.
2. Die Produktinformationen, insbesondere die Funktionsweise, der Umfang und die technischen Details der MDM/MAM-Lösung werden in **Anlage 3** dieser Dienstvereinbarung beigefügt. Die oder der Beschäftigte hat darüber hinaus das Recht, jederzeit Auskunft über die Art, den Umfang und die konkrete Funktionsweise der hierbei eingesetzten Software von der IT-Abteilung zu erhalten.
3. Die Bereitstellung der Anwendung erfolgt durch die Administratoren der IT-Abteilung des Bistums Limburg. Der Dienstgeber hat das Recht, Erweiterungen und Ergänzungen während der Laufzeit dieser Dienstvereinbarung einzusetzen. Die Beteiligungsrechte der Haupt-MAV/DiAG (besonders im Falle von Funktionserweiterungen) sind dabei zu beachten (siehe Abschnitt D § 23) und werden durch diese Dienstvereinbarung nicht eingeschränkt.
4. Der Auswahlprozess und die Entscheidung für den MDM/MAM-Anbieter, mithin der Anwendung für die Trennung dienstlicher und privater Daten sowie der Verwaltung von mobilen (dienstlichen) Applikationen, fanden unter Beteiligung und Mitsprache der Haupt-MAV/DiAG statt.

B. Nutzung dienstlicher und privater Endgeräte

§ 5 Dienstgeräte und Auswahl der Mitarbeiter

1. Die Auswahl und Ausstattung der Dienstgeräte liegt im Ermessen des Arbeitgebers. Die Entscheidung, welche oder welcher Beschäftigte ein Dienstgerät zur Verfügung gestellt bekommt, liegt allein im Ermessen des jeweiligen Arbeitgebers.
2. Für den Abschluss, die Verlängerung, Änderung und Kündigung etwaiger Mobilfunk- und Datenverbindungsverträge, die Auswahl der dazugehörigen Tarife sowie die bereitgestellte Hard- und Software ist im Hinblick auf die dienstlichen Endgeräte ebenfalls der jeweilige Arbeitgeber zuständig.

§ 6 Private Endgeräte und Auswahl der Beschäftigten

1. Die Entscheidung, welche oder welcher Beschäftigte sein privates Endgerät zu dienstlichen Zwecken nutzen kann und welche Endgeräte hierfür zugelassen werden, liegt im Ermessen des Arbeitgebers und gilt vorbehaltlich der Unterzeichnung der Einwilligungserklärung Mobiles Arbeiten (Anlage 2).

2. Für den Abschluss, die Verlängerung, Änderung und Kündigung etwaiger Mobilfunk- und Datenverbindungsverträge, die Auswahl der dazugehörigen Tarife sowie die bereitgestellte Hard- und Software ist im Hinblick auf die privaten Endgeräte die oder der Beschäftigte zuständig.

3. Der Einsatz und die Nutzung des privaten Endgerätes für dienstliche Zwecke stellt eine freiwillige Leistung des Arbeitgebers dar. Die Beschäftigten haben daher keinen Rechtsanspruch darauf, private Endgeräte für dienstliche Zwecke zu verwenden. Es besteht im Gegenzug auch keine Verpflichtung der Beschäftigten zur Nutzung privater Endgeräte zu dienstlichen Zwecken und damit zum Einsatz der MDM/MAM-Lösung.

4. Die Veröffentlichung der Mobilfunknummer des dienstlich genutzten privaten Endgerätes in einem Telefonverzeichnis bedarf der Zustimmung der oder des Beschäftigten.

§ 7 Pflichten der Beschäftigten

1. Bei der Nutzung der dienstlichen Endgeräte oder der Nutzung privater Endgeräte innerhalb der MDM/MAM-Lösung auf dem privaten Endgerät und dem Umgang mit dienstlichen Informationen sind die Interessen des Arbeitgebers nicht zu beeinträchtigen. Zu den nicht gestatteten Nutzungen zählen insbesondere, aber nicht abschließend:

   a) die wissentliche Preisgabe oder Gefährdung von dienstlichen- oder kirchlichen Geheimnissen, personenbezogenen Daten oder sonstigen Informationen des Arbeitgebers, die als vertraulich gekennzeichnet sind oder bei denen sich die Vertraulichkeit aus der Natur der Information ergibt;
   b) Abruf, Anbieten, Verbreiten oder Speichern von Inhalten, die gegen das Persönlichkeitsrecht, Urheberrecht, Datenschutzrecht oder Strafrecht verstoßen, insbesondere das unerlaubte Herunterladen oder Anbieten von Musik, Filmen, Software oder anderen urheberrechtlich geschützten Inhalten;
   c) Abruf, Anbieten, Verbreiten oder Speichern von rufschädigenden, beleidigenden, verleumderischen, diskriminierenden, menschenverachtenden, rassistischen, verfassungsfeindlichen, sexistischen, gewaltverherrlichenden oder pornografischen Inhalten;
   d) Abruf, Anbieten, Verbreiten oder Speichern von Computerviren oder anderer Malware sowie sonstige Aktivitäten, die sich gegen die Sicherheit von IT-Systemen richten (z. B. Hacking, Portscans);

2. Bei Verlust des dienstlichen oder des auch dienstlich genutzten privaten Endgerätes und im Falle eines Defektes ist die IT-Abteilung des Bistums Limburg und der Arbeitgeber unverzüglich zu informieren. Gleiches gilt bei der ersatzlosen Beendigung des Vertragsverhältnisses zwischen der oder dem Beschäftigen und einen Anbieter/Provider.

3. Im Hinblick auf die Nutzung der dienstlichen sowie der auch dienstlich genutzten privaten Endgeräte findet die Passwort- und Sicherheitsrichtlinie des Bistums in der jeweils aktuellen Fassung vollumfänglich Anwendung.

4. Dienstgeräte, die nicht mehr benötigt oder durch neue Geräte ersetzt werden, sind inklusive allem Zubehör an den Arbeitgeber zurückzugeben.

5. Eine erteilte Zustimmung zur Nutzung von dienstlichen oder privaten Endgeräten kann von Seiten des Arbeitgebers jederzeit widerrufen werden. Der Beschäftigte kann die dienstliche Nutzung des privaten Endgeräts jederzeit einstellen, vgl. Abschnitt C § 16.

§ 8 Telefon- und Datennutzung bei Dienstgeräten

1. Das dienstliche Endgerät darf nur innerhalb von Deutschland für dienstliche Kommunikation (Sprache, SMS und Daten) genutzt werden. Die Nutzung im Ausland bedarf der vorherigen Genehmigung durch den Arbeitgeber. Der Mitarbeiter muss Datendienste im Ausland deaktivieren. Falls der Mitarbeiter durch die Nutzung von Datendiensten im Ausland Kosten verursacht, kann der Arbeitgeber die Erstattung der hierbei anfallenden Kosten von der oder dem Beschäftigten fordern. Bei Mitarbeitern, die regelmäßig dienstlich im Ausland tätig sind, kann eine von dieser Regelung abweichende Absprache zwischen Arbeitgeber und Mitarbeiter erfolgen.
2. Die private Nutzung des dienstlichen Endgerätes ist nicht zulässig, es sei denn,
   a) es handelt sich um Notfälle (z. B. Telefonate aufgrund von Erkrankung von Familienangehörigen oder bei Unfällen),
   b) der Arbeitgeber erteilt hierzu vorab die Zustimmung oder
   c) die Privatnutzung ist aufgrund gesonderter schriftlicher Vereinbarung gemäß **Anlage 5** zwischen dem Arbeitgeber und der oder dem Beschäftigten vereinbart.

   In diesen Fällen bleibt die private Nutzungsmöglichkeit stets eine freiwillige, vom Arbeitgeber jederzeit widerrufbare Leistung.
3. Der Arbeitgeber ist berechtigt, von der oder dem Beschäftigten Nachweise darüber zu verlangen, ob die private Nutzung notfallbedingt veranlasst war.

§ 9 E-Mail und Internetzugang bei Dienstgeräten

1. Internetzugang
   a) Der im Zusammenhang mit dem jeweiligen Endgerät bereitgestellte Internetzugang steht den Beschäftigten als Arbeitsmittel im Rahmen ihrer dienstlichen Aufgabenerfüllung allein zu dienstlichen Zwecken zur Verfügung.
   b) Die private Nutzung des Internetzugangs ist unzulässig, es sei denn, die Privatnutzung ist aufgrund gesonderter schriftlicher Vereinbarung zwischen dem Arbeitgeber und der oder dem Beschäftigten vereinbart.
2. E-Mail
   a) Der dienstliche E-Mail-Account bzw. die der oder dem Beschäftigten von der IT-Abteilung zugewiesene E-Mail-Adresse dürfen ausschließlich für dienstliche Zwecke, bzw. zum dienstlichen Gebrauch genutzt werden. Die private Nutzung, mithin der Empfang und das Versenden von privaten E-Mails über den dienstlichen E-Mail-Account, ist untersagt.
   b) Bei einem Empfang rein privater E-Mails auf dem dienstlichen E-Mail-Konto sind diese unverzüglich von dort zu entfernen. Der Mitarbeiter hat das Recht, diese privaten E-Mails im Bedarfsfall zuvor auf ein privates E-Mail-Konto weiterzuleiten.

§ 10 Filter und Protokollierungen

1. Der E-Mail-Zugang sowie der Internetzugang innerhalb der MDM/MAM-Lösung dienen ausschließlich der dienstlichen Nutzung. Der Arbeitgeber ist daher berechtigt, die Nutzung vom E-Mail- und Internetzugang durch Einsatz von Filtersystemen zu beschränken (z.B. Sperren bestimmter Adressen oder Dateitypen, Domains, URLs, Dienste/Protokolle, Filesharing, Streaming, Ports) sowie Spam- und Virenfiltern einzusetzen.
2. Im Hinblick auf den dienstlichen E-Mail-Zugang und der eingesetzten MDM/MAM-Lösung ist der

Arbeitgeber auch berechtigt, die Annahme von E-Mails einzelner Absender, Gruppen von Absendern oder Domains zu verweigern. Die Nutzung des E-Mail- und Internetzugangs innerhalb der MDM/MAM-Lösung wird aus Gründen der Daten- und Systemsicherheit und zur Fehleridentifikation ebenfalls protokolliert und gespeichert.

a) Eine Unterscheidung zwischen privater und dienstlicher Nutzung innerhalb der MDM/MAM-Lösung ist damit aus technischen Gründen nicht möglich. Die Protokollierung erfolgt insbesondere mit Datum/Uhrzeit, genutztem Dienst (z. B. E-Mail, HTTP), Daten von Absender und Empfänger (z. B. IP-Adressen, Namen der Rechner, E-Mail-Adressen), gegebenenfalls Benutzerdaten (z. B. Benutzername bei E-Mail-Versand oder bei Einsatz eines Proxy-Servers), gegebenenfalls URLs der aufgerufenen Websites, technischen Statuscodes und übertragener Datenmenge.
b) Die Protokolle werden nach sechs (6) Monaten gelöscht, soweit nicht eine längere Speicherung im Einzelfall aus Gründen der Daten- und Systemsicherheit oder zur Fehleridentifikation und -behebung erforderlich ist.
c) Die Protokolle werden durch die IT-Abteilung des Bistums Limburg regelmäßig stichprobenhaft hinsichtlich der aufgerufenen Websites gesichtet und ausschließlich zu Zwecken der Gewährleistung/Wiederherstellung der Systemsicherheit, Analyse und Korrektur technischer Fehler und Störungen, Kapazitätsplanung und Lastverteilung sowie Optimierung der IT-Infrastruktur, statistischen Feststellung des Nutzungsumfangs, Missbrauchskontrolle und -verfolgung sowie bei Verdacht auf eine Straftat verwendet.

3. Der Zugriff auf diese Protokolldateien zum Zwecke der Erstellung der Übersicht und der jeweiligen Auswertung ist auf die Mitarbeiter des Referats Infrastruktur der IT-Abteilung des Bistums Limburg begrenzt. Die zugriffsberechtigten Personen sind in der **Anlage 4** zu dieser Dienstvereinbarung mit Namen, Vornamen, Dienststelle und Aufgabenbeschreibung aufgeführt. Diese Anlage ist bei Veränderungen zu aktualisieren. Jede Vertragspartei hat das Recht, im Einvernehmen mit der anderen Vertragspartei den benannten Personen das Zugriffsrecht aus wichtigem Grund zu entziehen. Das notwendige Einvernehmen der Parteien ist unverzüglich herzustellen.

4. Die Beteiligungsrechte der Haupt-MAV/DiAG und der zuständigen MAV bleiben auf jeden Fall unberührt. Jedwede Überwachung zur Verhaltens- und Leistungskontrolle der Beschäftigten (einschließlich einer ggf. technisch möglichen Ortung mittels der MDM/MAM-Lösung) ist unzulässig.

§ 11 Missbrauchskontrolle

1. Eine generelle Überwachung der Nutzung privater und dienstlicher Endgeräte, einschließlich der Telefon- und Datennutzung (E-Mail- und Internet) findet nicht statt. Der Fall des durch konkrete Tatsachen begründeten Verdachts von Straftaten in dienstlichem Zusammenhang oder einer unerlaubten Nutzung der elektronischen Informations- und Kommunikationsmittel, rechtfertigt eine Überprüfung der gespeicherten Daten sowie der aufgerufenen Web-Adressen im Sinne einer Missbrauchskontrolle innerhalb der MDM/MAM-Lösung unter Beteiligung der zuständigen Mitarbeitervertretung und eines in Abschnitt B § 10 Abs. 3 genannten Mitarbeiters.

2. Vor einer Missbrauchskontrolle hat der Arbeitgeber die zuständige MAV zu informieren. Eine weitere Beteiligung der zuständige MAV erfolgt nach den Vorschriften der MAVO. Ist ein MAV-Mitglied betroffen, wird die zuständig MAV als Gremium informiert; die weiteren Schritte sind mit einem von der zuständigen MAV beauftragten Mitglied abzustimmen.

3. Die Missbrauchskontrolle erfolgt unter unverzüglicher Beteiligung der oder des zuständigen betrieblichen Datenschutzbeauftragten im Rahmen der kirchlichen Datenschutzordnung (KDO).

4. Sofern sich ein konkreter Verdacht nicht bestätigt, sind die gewonnenen Daten unverzüglich, spätestens innerhalb von zehn (10) Kalendertagen unwiderruflich aus den aktiven Systemen zu löschen, bzw. zu vernichten. Ein Zugriff auf die so gelöschten oder vernichteten Daten in den Back-

Up-Systemen ist nicht gestattet. Die oder der Beschäftigte ist vom Dienstvorgesetzten oder dem beauftragten Mitglied der zuständigen MAV darüber zu informieren, welcher Verdacht, aufgrund welcher konkreten Tatsachen bestand und welche der ihm oder ihr zur Verfügung stehendenden Geräte von der Missbrauchskontrolle betroffen waren.

C. MDM/MAM-Lösung und private Endgeräte

§ 12 Umfang der Datenverarbeitung

1. Der Arbeitgeber erhält das Recht und die oder der Beschäftigte erteilt hierzu die Zustimmung, mit Hilfe der IT-Abteilung auf dem Endgerät der oder des Beschäftigten innerhalb des hierfür von der IT-Abteilung eingerichteten Containers, dienstliche Daten und Applikationen zu speichern, zu bearbeiten und zu löschen.
2. Der Arbeitgeber hat jederzeit das Recht, mit Hilfe der IT-Abteilung die dienstlichen Daten innerhalb des Containers zu lesen, zu ändern, hierauf zuzugreifen und bei Bedarf zu löschen. Der Arbeitgeber ist verpflichtet, insbesondere personenbezogene Daten, die im Zusammenhang mit dem Arbeitgeber stehen und sich im hierfür eingerichteten Container befinden, auf dem Endgerät der oder des Beschäftigten zu löschen, z. B. wenn ihre Speicherung Bestimmungen der KDO widerspricht, diese Daten vor Schadsoftware oder Malware geschützt werden müssen oder das Endgerät verloren oder gestohlen wurde. Zu diesem Zweck kann der Container im Wege des Remote-Wipe auch gelöscht oder der Zugang zur dienstlichen „Citrix-Oberfläche“ gesperrt werden.
3. Im Übrigen werden keine Daten des Arbeitgebers auf dem privaten Endgerät durch den Arbeitgeber verarbeitet. Ein Zugriff, Einsichtnahme oder Bearbeitung von privaten Daten der oder des Beschäftigten außerhalb des Containers, bzw. auf dem privaten Endgerät ist ausgeschlossen.

§ 13 Lizenzrechtliche Bestimmungen

1. Vom Dienstgeber bereitgestellte oder lizenzierte Software darf ausschließlich für dienstlicher Zwecke und in dem bereitgestellten Container betrieben werden. Dienstlich erworbene Softwarelizenzen verbleiben im Eigentum des Dienstgebers. Bei Beendigung oder Kündigung dieser Dienstvereinbarung, bzw. bei Beendigung der Rechte und Pflichten der oder des Beschäftigten gemäß dieser Dienstvereinbarung, ist die im Rahmen der dienstlichen Nutzung installierte oder bereit gestellte Software entsprechend der jeweils gültigen Lizenzbestimmungen zu deinstallieren oder kann vom Dienstgeber gelöscht werden.
2. Die Beschäftigten haben bei der Installation und Nutzung von Apps, die nicht über den App-Store des MDM/MAM-Anbieters oder durch die IT-Abteilung bereitgestellt werden, die lizenzrechtlichen Vorgaben gesondert zu beachten. Es wird darauf hingewiesen, dass die dienstliche Nutzung von privaten Apps und Softwares urheberrechtliche Konsequenzen sowohl für den Arbeitgeber, als auch die oder den Beschäftigten nach sich ziehen kann.

§ 14 Archivierung

1. Der Arbeitgeber unterliegt Archivierungs- und Aufbewahrungspflichten im Hinblick auf dienstliche Daten. Es gelten daher die Anordnungen über die Sicherung und Nutzung der Archive der katholischen Kirche sowie die Dienstanweisung zur Archivierung in der jeweils gültigen Fassung.
2. Vor der Löschung nicht mehr benötigter dienstlicher Daten (z.B. E-Mails) ist insbesondere zu prüfen, ob diese nicht den Aufbewahrungsfristen und einer Archivierungspflicht unterliegen. Im Zweifel

oder im Falle von Unklarheiten muss der Mitarbeiter vorab Rücksprache mit dem Arbeitgeber halten.

§ 15 Leistungs- und Verhaltenskontrolle

1. Der Einsatz und die Nutzung der MDM/MAM-Lösung zur Leistungs- und Verhaltenskontrolle sind in jedem Fall untersagt.
2. Erlangte Informationen über das Verhalten von Beschäftigten werden nicht zum Nachteil der betroffenen Beschäftigten verwendet.

§ 16 Beendigung und Herausgabe der dienstlichen Daten

1. Der Arbeitgeber sowie die oder der Beschäftigte können den Einsatz der MDM/MAM-Lösung jederzeit beenden.
2. Im Falle der Beendigung des Arbeits-, Dienst- und Vertragsverhältnisses mit der oder dem Beschäftigten durch Kündigung oder Beendigung - gleich von welcher Seite und aus welchem Grund - Zeitablauf, Aufhebungsvertrag oder gerichtliche Entscheidung - ist die oder der Beschäftigte verpflichtet, die dienstlichen Daten, die auf dem Endgerät vorhanden und nicht mit den Servern des Dienstgebers synchronisiert worden sind, an den Arbeitgeber herauszugeben.
3. Der Arbeitgeber kann von der oder dem Beschäftigten die schriftliche Versicherung verlangen, wonach sämtliche dienstlichen Daten auf dem privaten Endgerät unwiederbringlich gelöscht worden sind. Ein Zurückbehaltungsrecht der oder des Beschäftigten an den dienstlichen Daten, gleich aus welchem Grund, ist ausgeschlossen.

§ 17 Kostenübernahme

1. Die Kostenerstattung durch den Arbeitgeber für die dienstliche Nutzung des privaten Endgerätes erfolgt pauschal mit einer monatlichen Zahlung in Höhe von 25,00 € (brutto), die über die Gehaltsabrechnung abgeführt wird. Mit dieser Zahlung sind sämtliche Leistungen der oder des Beschäftigten im Zusammenhang mit der dienstlichen Nutzung des privaten Endgerätes abgegolten. Der Anspruch auf Kostenerstattung entsteht ab dem Monat, in dem die MDM/MAM-Lösung installiert wird.
2. Der Arbeitgeber und die oder der Beschäftigte werden für den Fall, dass aufgrund eines erheblichen dienstlichen Datenaufkommens Zusatzkosten entstehen, eine entsprechende Anpassung der Zahlung vereinbaren.
3. Die Kostenerstattung gilt befristet bis zum Ablauf oder der Kündigung dieser Dienstvereinbarung, dem Widerruf der oder des Beschäftigten, bzw. des Arbeitgebers oder der ersatzlosen Beendigung des Vertragsverhältnisses zwischen der oder dem Beschäftigten und dem Anbieter/Provider, je nachdem, welches Vertragsverhältnis früher endet. Der Anspruch auf Kostenerstattung erlischt mit Ablauf des Monats, in dem ein Ereignis nach Satz 1 eintritt.
4. Die oder der Beschäftigte überlässt dem Arbeitgeber bei Bedarf eine Kopie der Vertragsurkunde mit dem Anbieter/Provider.
5. Wechselt die oder der Beschäftigte von einem dienstlichen Endgerät zu einem privaten Endgerät mit dienstlicher Nutzung, besteht der Anspruch auf Zahlung der Zulage für die dienstliche Nutzung erst ab dem Zeitpunkt, zu dem der geschlossene Mobilfunkvertrag beendet worden oder auf eine andere Beschäftigte oder einen anderen Beschäftigen übergegangen ist. Der Arbeitgeber ist ver-

pflichtet, die oder den Beschäftigten zum frühestmöglichen Zeitpunkt einen Wechsel zu ermöglichen.

§ 18 Arbeits- und Dienstzeit

1. Die arbeitsrechtlich, bzw. dienstlich festgelegte, wöchentliche Arbeitszeit bleibt auch beim Einsatz der privaten Endgeräte zu dienstlichen Zwecken unverändert. Die Bestimmungen des Arbeitszeitgesetzes und der AVO bleiben unberührt, soweit die oder der Beschäftigte unter diese Bestimmungen fällt.
2. Die Parteien sind sich darüber einig, dass alle dienstlichen Belange während der dienstüblichen Arbeitszeit erledigt werden sollen. Das Führen dienstlicher Telefonate oder die Beantwortung dienstlicher E-Mails am Abend oder am Wochenende stellt eine vorrübergehende Verlängerung der Arbeitszeit dar und bedarf der Abstimmung mit dem Arbeitgeber.
3. Wenn zur Aufrechterhaltung dringender dienstlicher Abläufe eine Erreichbarkeit des oder der Beschäftigten außerhalb der dienstüblichen Arbeitszeit trotzdem zwingend erforderlich ist, vereinbaren die oder der Beschäftigte und der Arbeitgeber einen abgegrenzten Rahmen zur mobilen Erreichbarkeit. Die Regelungen über den Bereitschaftsdienst und die Rufbereitschaft gemäß AVO bleiben unberührt. Die gesetzliche Ruhezeit ist nach Ende des Einsatzes mobiler Arbeitsmittel am Abend einzuhalten. Die Zeit, die die oder der Beschäftigte außerhalb der dienstüblichen Arbeitszeit für dienstliche Belange aufbringt, ist Arbeitszeit und mangels einer anderslautenden Regelung entsprechend zu vergüten.
4. Das Recht der Parteien, die Erreichbarkeit mittels technischer Einrichtung nach Dienstschluss (insbesondere mit Hilfe der MDM-Lösung) einzuschränken oder auszuschließen, bleibt unberührt.

§ 19 Haftung

1. Im Falle des Verlustes oder der Beschädigung des privaten Endgerätes der oder des Beschäftigten, die durch eine Handlung des Arbeitgebers, seiner gesetzlichen Vertretung oder Erfüllungsgehilfen verursacht worden ist, haftet der Arbeitgeber gegenüber der oder dem Beschäftigten nach den gesetzlichen Bestimmungen.
2. Der Arbeitgeber haftet darüber hinaus für Schäden der oder des Beschäftigten, die dieser nachweislich im Zusammenhang mit der dienstlichen Nutzung seines privaten Endgerätes durch eine nicht grob fahrlässige oder vorsätzliche Handlung der oder des Beschäftigten an dem Endgerät erleidet. Der Arbeitgeber haftet ebenso für Schäden, die der oder die Beschäftigte im Rahmen ihrer oder seiner dienstlichen Tätigkeit bei Dritten verursacht und dieses nicht grob fahrlässig ist.
3. Im Falle des Verlustes, der Beschädigung oder Wertminderung des privaten Endgerätes der oder des Beschäftigten, die durch vorsätzliche oder grob fahrlässige Handlungen der oder des Beschäftigten selbst verursacht werden (auch soweit diese durch mangelhafte Pflege oder Wartung sowie durch unterlassene Reparaturen entstehen), haftet die oder der Beschäftigte ebenso selbst, wie im Zusammenhang mit der reinen Privatnutzung.
4. Bei einer unbefugten Überlassung des privaten Endgerätes an eine dritte Person haftet die oder der Beschäftigte für jeden hierdurch entstehenden Schaden, unabhängig von eigenem Verschulden. Gleiches gilt für Schäden, die in diesem Fall Dritten zugefügt werden. Bei einer Überlassung des privaten Endgeräts an eine dritte Person hat der Beschäftigte sicherzustellen, dass diese in keiner Weise Zugriff auf dienstliche Vorgänge oder Daten erlangen kann.
5. Die Haftung die oder des Beschäftigten wird eingeschränkt oder entfällt, soweit eine Versicherung für den Schaden aufkommt und nicht auf den Arbeitgeber Rückgriff genommen wird.

§ 20 Ersatzbeschaffung und Wartung

1. Im Falle des Verlustes, der Zerstörung oder eines technischen Defektes des privaten Endgerätes, ist die oder der Beschäftigte nicht verpflichtet, sich erneut ein gleichwertiges Endgerät zur Erbringung ihrer oder seiner dienstlichen Aufgaben anzuschaffen.
2. Die oder der Beschäftigte ist für die Wartung und Pflege des privaten Endgerätes selbst verantwortlich. Die Kosten für Reparaturen und für Instandsetzungen des Endgerätes sind von der oder dem Beschäftigten zu tragen.
3. Die IT-Abteilung leistet mit Ausnahme auf die MDM/MAM-Lösung keinen technischen Support im Hinblick auf das private Endgerät.

§ 21 Steuerliche Vorteile

Die Übernahme eines Anteils der monatlichen Kosten oder der Bezuschussung des privaten Endgerätes, stellen u. U. einen steuerpflichtigen Sachbezug (geldwerter Vorteil) dar. Es sind die jeweils gültigen steuer- und sozialversicherungsrechtlichen Gesetze und Vorschriften zu berücksichtigen.

D. Gemeinsame Schlussbestimmungen

§ 22 Verschwiegenheitsverpflichtung

1. Bestehende Verschwiegenheitsverpflichtungen der Beteiligten nach Maßgabe der AVO bleiben unberührt und finden auf diese Dienstvereinbarung Anwendung.
2. Vertrauliche Informationen in diesem Sinne sind neben ausdrücklich als „vertraulich“ gekennzeichneten Informationen auch aus den Umständen erkennbar als vertraulich zu behandelnde Informationen, personenbezogene Daten der betroffenen Beschäftigten und insbesondere in Zusammenhang mit der Einsichtnahme in E-Mail-Accounts, Daten zur Nutzung von Internet-Accounts oder ggf. erlangte, private Informationen.

§ 23 Rechte und Beteiligung der Mitarbeitervertretung

1. Die Haupt-MAV/DiAG wird rechtzeitig vor ihrer Einführung umfassend über den Stand und die Umsetzung von wesentlichen neuen sowie geplanten Erweiterungen von bestehenden MDM-Lösungen sowie deren Auswirkungen auf die Mitarbeiter unterrichtet und nach Maßgabe der MAVO beteiligt.
2. Die Unterrichtungs- und ggf. Zustimmungspflicht bezieht sich insbesondere auf
   a) die organisatorischen und personellen Auswirkungen,
   b) die vorgesehenen Maßnahmen zu Datenschutz und Datensicherheit,
   c) die Auflistung der vorgesehenen Systemkomponenten, einschließlich geplanter Vernetzungen und Verknüpfungen.
3. Der Dienstgeber richtet einen Koordinierungsausschuss ein, der an der Planung, Koordinierung und organisatorischen Begleitung von Maßnahmen im Bereich der „MDM/MAM-Lösungen“ beteiligt ist. Die Haupt-MAV/DiAG nimmt beratend an den Sitzungen des Ausschusses teil. Richtet der Dienstgeber weitere Arbeitsgruppen ein, so ist die Haupt-MAV/DiAG berechtigt, auch an diesen Arbeitsgruppen beratend teilzunehmen. Eine von der Haupt-MAV/DiAG benannte Vertretung hat in Begleitung einer oder eines IT-Verantwortlichen des Dienstgebers Zugang zu den technischen

Einrichtungen und kann sich von der Einhaltung der Dienstvereinbarung - auch stichprobenweise - überzeugen. Eine entsprechende auch unangemeldete Zugangs- und Kontrollmöglichkeit ist vom Dienstgeber zu gewährleisten.

§ 24 Datenschutz

Bei der Verarbeitung und Speicherung von Daten, insbesondere personenbezogenen Daten, sind die Datenschutzvorschriften gemäß der Anordnung über den kirchlichen Datenschutz (KDO) und der hierzu ergangenen Durchführungsverordnung (KDO-DVO) zu beachten. Die Einsicht in und die Nutzung von erfassten Benutzerdaten dürfen ausschließlich von den zugriffsberechtigten Personen (Anlage 4) für Zwecke der Systemsicherheit und der Systemintegrität erfolgen.

§ 25 Folgen bei Verstößen

Verstöße gegen diese Dienstvereinbarung stellen Pflichtverletzungen des Arbeitsvertrages dar und können entsprechend sanktioniert werden.

§ 26 Änderungen und Ergänzungen

1. Auf Antrag einer der beiden Seiten findet eine Aussprache zu dieser Dienstvereinbarung statt.
2. Geplante Änderungen und Erweiterungen im Zusammenhang mit der MDM/MAM-Lösung werden der Haupt-MAV/DiAG mitgeteilt. Es wird dann geprüft, ob und inwieweit sie sich auf die Regelungen dieser Vereinbarung auswirken. Notwendige Änderungen oder Erweiterungen zu dieser Vereinbarung können im Einvernehmen in einer ergänzenden Regelung vorgenommen werden. Beteiligungsrechte und Mitwirkungsrecht der Haupt-MAV/DiAG bleiben unberührt.

§ 27 In-Kraft-Treten

1. Diese Vereinbarung tritt zum 01.05.2018 in Kraft und ersetzt die Dienstvereinbarung vom 01.01.2017. Sie ist erstmalig kündbar zum 31.12.2018. Im Falle der Kündigung verpflichten sich beide Vertragsparteien zur sofortigen Aufnahme zur Verhandlungen zu einer neuen Dienstvereinbarung zum gleichen Thema. Soweit diese Verhandlungen binnen eines Jahres nicht zum Abschluss einer neuen Dienstvereinbarung geführt haben, gilt diese Dienstvereinbarung noch ein weiteres Jahr fort und entfaltet anschließend keine Nachwirkung mehr.
2. Im Übrigen gelten die Bestimmungen der MAVO.
3. Die Dienstvereinbarung ist im Internet in der jeweils gültigen Fassung veröffentlicht.

Udo Koser
Vorsitzender der Haupt-MAV/DiAG

Wolfgang Rösch
Generalvikar

Anlage 1

1. Mit „Dienstgeber“ ist das Bistum Limburg als Verhandlungspartner der Haupt-MAV/DiAG gemeint. Demgegenüber ist „Arbeitgeber“ der Vertragspartner der oder des Beschäftigten, z.B. die Kirchengemeinde.
2. „Endgerät“ umfasst vorliegend die vom Bistum freigegebenen Smartphones und Tablets.
3. „Dienstliche Daten“ bedeutet alle Daten, die bei einem Arbeitgeber bzw. beim Bistum im Rahmen der elektronischen oder nicht-elektronischen Datenverarbeitung intern oder extern anfallen, mit denen das Bistum in Verbindung steht oder die sonst in Zusammenhang mit der dienstlichen, kirchlichen, mildtätigen oder gemeinnützigen Tätigkeit in Verbindung zu bringen sind.
4. Ein „geschäftlicher oder dienstlicher Gebrauch“ liegt dann vor, wenn die Nutzung der IT-Infrastruktur dienstlich veranlasst ist und die oder der Beschäftigte dadurch die Arbeit als Beschäftige des Bistums oder der Kirchengemeinde voranbringen will.
5. Von einer „Privatnutzung“ ist auszugehen, wenn der Gebrauch der IT-Infrastruktur durch die oder den Beschäftigten keinerlei dienstlichen Bezug vorweist und auch nicht der Erfüllung seiner arbeitsvertraglichen, bzw. dienstlichen Pflichten dient.
6. „Datenverarbeitung“ i. S. d. Vereinbarung bedeutet das Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten (§ 2 (4) KDO in ihrer Fassung zum Zeitpunkt der Erstellung der Dienstvereinbarung).
7. Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener) (§ 2 (1) KDO in ihrer Fassung zum Zeitpunkt der Erstellung der Dienstvereinbarung).
8. „Mobile Device Management“ bedeutet die zentrale Konfiguration und Verwaltung des Endgerätes.
9. Unter „Malware“ versteht man „bösartige“ Software (Computerprogramme), wie z. B. Computerviren, Computerwürmer, Trojaner und Back-Doors, die unerwünschte und ggf. schädliche Funktionen ausführen. Schadfunktionen können zum Beispiel die Manipulation oder das Löschen von Dateien oder das technische Kompromittieren der Sicherheitssoftware oder anderer Sicherheitseinrichtungen (wie z. B. Firewalls und Antivirenprogramme) der IT-Infrastruktur sein.
10. „Remote“ bedeutet den externen technischen Zugriff (oder technische Einflussnahme) auf das freigegebene Endgerät der oder des Beschäftigten oder auf das firmeneigene Rechnernetz des Bistums mittels einer Einstellung, Software oder Applikation. Der externe Zugriff kann hierbei per Intranet, (z. B. über ein lokales Netzwerk-LAN) oder auch per Internet oder VPN ermöglicht werden. Mit Hilfe dieses „Remote-Zugriffs“ kann die IT-Abteilung des Bistums auf Endgeräte der Beschäftigten oder umgekehrt, Beschäftigte auf das Rechennetz des Bistums zugreifen, Daten einsehen, bearbeiten und unter Umständen löschen.
11. „Remote-Wipe“ bedeutet selektives Löschen von Daten durch den externen Zugriff auf das Endgerät der oder des Beschäftigte, wodurch die dienstlichen Daten des Arbeitgebers gelöscht werden können.
12. „Datendienste“ Datendienste bieten dem Anwender die Möglichkeit, mit einem Mobiltelefon/Smartphone oder einem anderen Kommunikationsgerät u. a. auf Webseiten, E-Mail, Fax und SMS- bzw. Multimedia-Mitteilungen zuzugreifen. Die Nutzung von Datendiensten lässt sich in den Einstellungen des Mobiltelefons/Smartphones deaktivieren bzw. für die Nutzung in fremden Netzen blockieren.

Anlage 2

Bistum Limburg

Hiermit bestätige ich, _____ (Nachname, Vorname) den Inhalt der Dienstvereinbarung über den Einsatz und die Nutzung von „XenMobile" im Zusammenhang mit privaten und dienstlichen Endgeräten zur Kenntnis genommen zu haben. Ich erkläre hiermit mein Einverständnis mit der Geltung der in der Dienstvereinbarung getroffenen Regelungen in ihrer jeweils gültigen Fassung* im Hinblick auf den Einsatz meines genehmigten mobilen Gerätes.

Ich erkläre hiermit folgendes:

1. Der Dienstgeber darf im Rahmen der Dienstvereinbarung mein Endgerät in das Mobilgerätemanagement (MDM) und Management mobiler Anwendungen (MAM) von XenMobile aufnehmen. Die Funktionsweise wurde mir erläutert.
2. Im Hinblick auf den bereitgestellten Container können von Seiten der IT-Abteilung des Bistums Limburg Sicherheitseinstellungen vorgenommen und geändert werden und die Applikationen (Apps) innerhalb des Container durch die IT-Abteilung des Bistums Limburg kontrolliert werden.
3. Der Arbeitgeber bzw. die IT-Abteilung des Bistums Limburg im Auftrag des Arbeitgebers darf jederzeit auf alle in dem Container gespeicherten dienstlichen Inhalte und Daten zugreifen, diese ändern oder löschen.
4. Der Zugriff, Einsichtnahme, Veränderung oder Löschung von privaten Daten außerhalb des Containers ist nicht gestattet und ist ausgeschlossen.

Mir ist bekannt, dass ich meine Einwilligung jederzeit formlos gegenüber der dem Dienstgeber/Arbeitgeber widerrufen kann. In diesem Fall endet meine Befugnis zur Nutzung meines mobilen Gerätes zu dienstlichen Zwecken im Zeitpunkt des Widerrufs. Der Widerruf bedarf der Textform.

Ort, Datum	Unterschrift Mitarbeiter/in

Stand: Mai 2018

* https://formularsammlung.bistumlimburg.de/fileadmin/redaktion/Bereiche/Formularsammlung/downloads/DVMobilesArbeiten.pdf

Citrix Workspace Suite

Stellen Sie mit der neuen Citrix Workspace Suite auf jedem Endgerät sicheren Zugriff auf Anwendungen, Daten und Services bereit. Diese umfassende und leistungsstarke Lösung wurde entwickelt, um die Anforderungen eines jeden Anwenders hinsichtlich Performance, Sicherheit und Mobility zu erfüllen. Sie bietet sofortigen Zugriff auf benutzerspezifische Desktops, Apps, Web- und Windows-Anwendungen, Daten und Services über jedes Netzwerk.
Die Freiheit, selbst zu bestimmen, wie, wo und wann sie arbeiten, macht Mitarbeiter mobiler und produktiver.

Die Arbeitswelt hat sich verändert. Die Zeiten, in denen Mitarbeiter einfach in einem Firmenbüro mit einem unternehmenseigenen Gerät arbeiteten, sind vorbei. Die Mitarbeiter von heute arbeiten an den unterschiedlichsten Standorten, wie z. B. beim Kunden, in Fabrikhallen, Hotels oder zuhause – und das mit vielen verschiedenen Endgeräten. In der Tat verwenden Mitarbeiter mehr als drei verschiedene Endgeräte pro Tag, um ihre Arbeit zu erledigen. Prognosen von Analysten zufolge werden sich in den nächsten Jahren immer mehr Arbeitgeber darauf einstellen, dass ihre Mitarbeiter auch private Endgeräte (Laptops, Smartphones und Tablets) zur Arbeit nutzen. Das bedeutet, dass es Millionen von BYO-Endgeräten am Arbeitsplatz geben wird.

Vorteile der Citrix Workspace Suite

- Mehr Produktivität für Mitarbeiter durch sofortigen Zugriff auf Anwendungen, Daten und Desktops
- Hohe Performance über jedes beliebige Netzwerk
- Mehr Möglichkeiten für Mitarbeiter durch Self-Service-Zugriff auf Unternehmensressourcen
- Sichere Unternehmensdaten in der Cloud und auf dem Endgerät
- Eine zentrale, flexible Lösung für ein umfassendes Management

BYO-Endgeräte sind jedoch erst der Anfang. Obwohl Mobility zur Normalität geworden ist, sind Unternehmen den Anforderungen der Anwender nicht immer nachgekommen. Diese wollen Zugriff auf die neuesten und besten Anwendungen oder Unternehmensdaten auf jedem Endgerät und an jedem Ort. Stattdessen wurde in neue Technologien investiert, um taktische Herausforderungen anzugehen: gehostete Anwendungen für den Remote-Zugriff, virtuelle Desktops für externe Dienstleister oder Mobilgerätemanagement für unternehmenseigene Mobilgeräte. Diese Implementierungen wurden erweitert, sobald neue Anwendungsszenarien bzw. Anwenderanforderungen hinzukamen. Organisationen, die so vorgegangen sind, stehen nun vor dem Problem, dass sie mehrere teure Infrastrukturen implementiert haben, die jeweils ein spezielles Management, Support und Know-how erfordern.

Unternehmen müssen die Vorgehensweise überdenken, wie sie Desktops, Anwendungen, Daten und mobile Services an Mitarbeiter bereitstellen, die nicht immer im Büro sind und kein unternehmenseigenes Endgerät verwenden. Die ideale Lösung sollte Anwendungen, Desktops, Daten und Services nahtlos und sicher miteinander verbinden, um einen einfachen und sicheren Zugriff von überall zu bieten. Die Lösung besteht aus einem mobilen Arbeitsplatz, der einen Mitarbeiter an jeden Ort begleitet, unabhängig von verwendetem Endgerät und Netzwerk.

Die Citrix Workspace Suite passt sich schnell wechselnden Anforderungen an und ist die branchenführende Lösung für mobile Arbeitsplätze. Sie ermöglicht der IT, alle Anwendungen (Windows, Web, SaaS, Apps), Daten und Services von jedem Endgerät über jedes Netzwerk bereitzustellen, um Menschen die Möglichkeit zu eröffnen, besser zu arbeiten.

Hauptfunktionen

Benutzerspezifische Inhalte für jeden Anwender

Mitarbeiter von heute fordern Flexibilität, um mit jedem Endgerät und von überall aus arbeiten zu können. Mit der Citrix Workspace Suite können Mitarbeiter auf all ihre Anwendungen, Daten und sogar auf ihre benutzerspezifischen Desktops zugreifen – von jedem unternehmenseigenen oder BYO-Endgerät,darunter Tablets, Smartphones, PCs, Macs oder Thin Clients. Zudem kann die IT Anwendungen, Desktops und Daten individuell zusammenstellen und gleichzeitig Inhalte optimieren, um die Anforderungen jedes einzelnen Mitarbeiters an Sicherheit, Performance, Personalisierung und Mobility zu erfüllen.

„Mobile Arbeitsplätze finden immer häufiger ihren Weg in die Unternehmen und machen eine umfassende mobile Sicherheit unverzichtbar. Citrix Workspace Suite geht auf diese kritischen Anforderungen der Unternehmen ein und gibt der IT Sicherheit und Kontrolle. Gleichzeitig erhalten Mitarbeiter die Flexibilität, von überall und vom Endgerät ihrer Wahl aus zu arbeiten, mit Zugriff auf alle Anwendungen, Daten und Tools für die Zusammenarbeit, die sie benötigen

Mark Bowker
Senior Analyst
Enterprise Strategy Group

Self-Service-Zugriff auf alle Anwendungen

Citrix Workspace Suite bietet einen vereinheitlichten App-Store, der Windows-, Web-, SaaS-Anwendungen und mobile Apps zur Bereitstellung auf jedem beliebigen Endgerät bündelt. Mit dem App-Store kann die IT alle Services des Unternehmens an einem zentralen Ort hosten. Und alle Mitarbeiter erhalten einen Self-Service-Zugriff auf die Anwendungen, die sie für produktives Arbeiten benötigen. Zusätzlich enthält Citrix Workspace Suite native mobile Apps für sichere E-Mail-, Kalender- und Browserfunktionen und ermöglicht mobilen Mitarbeitern somit ein Maximum an Produktivität und Sicherheit.

Größter Benutzerkomfort

Citrix Workspace Suite bietet den höchsten Komfort für die Nutzung jeder beliebigen Anwendung und jedes beliebigen Desktops. Mithilfe eines universellen Clients, der auf allen Tablets, Smartphones, PCs, Macs oder Thin Clients verfügbar ist, kann die IT Windows-Anwendungen mit hoher Performance über WANs mit geringer Bandbreite und hoher Latenz, hochvariable mobile 3G/4G-Netzwerke oder ein verlässliches Firmen-LAN bereitstellen. Die IT kann Web-, SaaS-Anwendungen und mobile Apps auf jedem mobilen Endgerät mit einem beispiellosen Benutzerkomfort sicher bereitstellen. Gemeinsam bieten diese Technologien den Mitarbeitern die beste Basis für hervorragende Leistungen.

Secure by Design

Die Citrix Workspace Suite schützt Daten und Anwendungen mit einer umfassenden Sicherheitsarchitektur, die die Einhaltung gesetzlicher Vorgaben gewährleistet. Mitarbeiter können über jedes Endgerät auf all ihre Daten zugreifen, diese synchronisieren und sie auf sichere Weise an Menschen innerhalb und außerhalb des Unternehmens senden. Zusätzlich verfügt die IT über die Flexibilität, Daten im eigenen Rechenzentrum, in der Cloud oder einem Mix aus beidem zu managen, wodurch ein effizienter Betrieb ermöglicht wird. Organisationen können mithilfe der Zentralisierung der Anwendungen und Desktops, durch die alle Daten im Rechenzentrum verbleiben, das Risiko für den Verlust von geistigem Eigentum und vertraulichen privaten Informationen minimieren. Zu guter Letzt kann die IT die mobilen Apps mit Funktionen wie Datenverschlüsselung, Passwort-Authentifizierung, sicherem Sperren und Löschen, App-interne Richtlinien und Mikro-VPNs erweitern, um die Sicherheit der Daten auf dem Endgerät noch weiter zu vergrößern.

Eine zentrale, flexible Lösung

Die unterschiedlichen Anforderungen von heutigen Mitarbeitern führten zwangsweise zu einer Vielzahl von Infrastrukturen für Desktops, Mobilgeräte, Anwendungen und Daten. Jede davon muss individuell gemanagt und gewartet werden. Citrix Workspace Suite nimmt dieses Problem in Angriff und bietet eine umfassende, flexible Lösung, die die Anwendungs- und Desktop-Bereitstellung sowie das Lifecycle-Management optimiert und so IT-Kosten spart. Durch das zentrale Management und die Bereitstellung von Standard-Images nach Bedarf kann die IT Anwendungs- und Desktop-Images einfach updaten und rollenbasiertes Management, Konfiguration, Sicherheit und Support für firmen- und mitarbeitereigene Geräte bereitstellen.

Corporate Headquarters
Fort Lauderdale, FL, USA

Silicon Valley Headquarters
Santa Clara, CA, USA

EMEA Headquarters
Schaffhausen, Schweiz

India Development Center
Bangalore, Indien

Online Division Headquarters
Santa Barbara, CA, USA

Pacific Headquarters
Hongkong, China

Latin America Headquarters
Coral Gables, FL, USA

UK Development Center
Chalfont, Großbritannien

Über Citrix

Citrix (NASDAQ:CTXS) ist ein Anbieter von Virtualisierungs-, Netzwerk- und Cloud Computing-Infrastruktur, die Menschen bei neuen Formen der Zusammenarbeit unterstützt. Citrix-Lösungen helfen IT-Abteilungen und Service Providern beim Aufbau der Verwaltung und der Absicherung virtueller und mobiler Arbeitsplätze. Damit lassen sich einzelne Anwendungen oder gesamte Desktops sowie Daten und Dienste jederzeit auf jedem Endgerät und über jedes Netzwerk oder Cloud bereitstellen. Bereits seit 25 Jahren ermöglicht Citrix mit innovativen Produkten die Umsetzung flexibler und mobiler Arbeitsmodelle. Mehr als 330.000 Unternehmen und über 100 Millionen Anwender setzen weltweit auf Technologie von Citrix. Der jährliche Umsatz in 2013 betrug 2,9 Milliarden US-Dollar. Weitere Informationen unter www.citrix.de.

Anlage 4

Zugriffsberechtigte Beschäftigte des Referates Infrastruktur der IT-Abteilung des Bistums Limburg

1. Weck, Andreas — Leiter des Referates Infrastruktur, stellv. Abteilungsleiter
   E-mail: a.weck@it.bistumlimburg.de
   Tel.: 06431 295-172

2. Dasbach, Sebastian — IT-Sachbearbeiter im Referat Infrastruktur
   E-Mail: s.dasbach@it.bistumlimburg.de
   Tel.: 06431 295-470

3. Hilb, Julian — IT-Sachbearbeiter im Referat Infrastruktur
   E-Mail: j.hilb@it.bistumlimburg.de
   Tel.: 06431 295-176

4. Schardt, Harald — IT-Sachbearbeiter im Referat Infrastruktur
   E-Mail: h.schardt@it.bistumlimburg.de
   Tel.: 06431 295-433

5. Wagner, Matthias — IT-Sachbearbeiter im Referat Infrastruktur
   E-Mail: m.wagner@it.bistumlimburg.de
   Tel.: 06431 295-553

Anlage 5

Bistum Limburg

Einwilligungserklärung zur privaten Nutzung des dienstlichen Internet- und E-Mail-Zugangs

Ich willige ein, dass der Arbeitgeber bzw. die IT-Abteilung des Bistums Limburg im Auftrag des Arbeitgebers aus Gründen der Daten- und Systemsicherheit, zur Fehleridentifikation und -behebung sowie zur Verfolgung von Straftaten meine private Nutzung des dienstlichen E-Mail- und Internetzugangs protokolliert und auswertet. Eine Unterscheidung zwischen privater und dienstlicher Nutzung innerhalb der MDM/MAM-Lösung ist aus technischen Gründen nicht möglich. Der Dienstgeber ist berechtigt, die Nutzung von E-Mail- und Internetzugang insbesondere durch Einsatz von Filtersystemen zu beschränken, z. B. in Form von Sperren bestimmter Adressen (z. B. Domains, URLs), Dienste/Protokolle (z. B. Filesha-ring, Streaming) oder Ports, der Einsatz von inhaltsbasierten Filtersystemen (z. B. Sperrung bestimmter Schlagwörter oder Dateitypen) sowie der Einsatz von Spam- und Virenfiltern.

Ich befreie den Arbeitgeber zudem vom Fernmeldegeheimnis nach § 88 TKG und allen damit verbundenen Beschränkungen, soweit es meine private Nutzung des dienstlichen E-Mail- und Inter-netzugangs betrifft.

Diese Einwilligung ist freiwillig. Erteile ich sie nicht, entstehen mir keine weiteren Nachteile als dass ich den dienstlichen Internetzugang nicht privat nutzen darf. Ich kann diese Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen. Ab meinem Widerruf entfällt die Berechtigung zur privaten Nutzung des dienstlichen Internet- und E-Mail-Zugangs ebenfalls für die Zukunft. Ein Widerruf der Einwilligung ist ausgeschlossen, soweit er sich auf Daten und Informationen bezieht, die vor dem Widerruf entstanden sind. Damit bleibt der Dienstgeber insbesondere auch nach einem Widerruf vom Fernmeldegeheimnis befreit, soweit der Zeitraum vor meinem Widerruf betroffen ist und kann die vorgenannten Kontrollen durchführen und Konsequenzen bei Verstößen ziehen.

Ich weise den Arbeitgeber zudem an, nach meinem Ausscheiden bei dem Arbeitgeber auf meinem dienstlichen E-Mail-Zugang eingehende und gespeicherte Nachrichten privaten Charakters zu löschen bzw. durch die IT-Abteilung beim Bistum Limburg löschen zu lassen. Ich verpflichte mich, für die Privatnutzung des Dienstgerätes eine Pauschale in Höhe von monatlich 15,00 € an den Arbeitgeber zu entrichten. Der Betrag wird vom Nettogehalt einbehalten. Die Pauschale ist ab dem Kalendermonat nach Antragstellung zu zahlen. Wird die Einwilligung widerrufen, endet die Zahlungspflicht mit dem Ende des Monats, in dem die Berechtigung zur privaten Nutzung entfällt.

Im Übrigen gelten die Bestimmungen der Dienstvereinbarung über den Einsatz und die Nutzung von „XenMobile" im Zusammenhang mit privaten und dienstlichen Endgeräten in der jeweils gültigen Fassung* auf die mit dieser Einwilligungserklärung verwiesen wird.

Ort, Datum

Unterschrift Mitarbeiter/in

Stand: Mai 2018

* https://formularsammlung.bistumlimburg.de/fileadmin/redaktion/Bereiche/Formularsammlung/downloads/DVMobilesArbeiten.pdf