ABl 15/2014, S. 552-567

Richtlinie für die Benutzung von Arbeitsplatzcomputern (APC) in der Diözese Augsburg (Stand 01.12.2014)

1. Präambel

Der Einsatz von Computern, mobilen Geräten und Software für die Erledigung der täglichen Arbeit ist in allen Stellen im kirchlichen Bereich eine Selbstverständlichkeit geworden.

Die Beachtung dieser Richtlinie ist erforderlich, um die Funktionsfähigkeit und die Sicherheit der Systeme zu gewährleisten und einen wirtschaftlichen Einsatz der APC's zu erreichen.

2. Begriffsbestimmung

Arbeitsplatzcomputer (APC) im Sinne dieser Richtlinie sind alle Hard- und Softwaresysteme (z.B. vernetzte und nicht vernetzte stationäre Personalcomputer, Workstations und Terminals, sowie alle mobilen Geräte [Notebooks, Laptops, Palmtops, Webbooks, Smartphones u.a.m.]) der elektronischen Datenverarbeitung (EDV), die einem Benutzer zur Erfüllung seiner dienstlichen/ehrenamtlichen Aufgaben von einem kirchlichen Rechtsträger (insbesondere Diözese Augsburg, Pfarrkirchenstiftungen etc.) zur Verfügung gestellt werden.

Des Weiteren gelten als APC's, alle Hard- und Softwaresysteme, welche von der Betreuungseinheit betreut werden.

Als zuständige ***Betreuungseinheit*** gilt

- die Abteilung Organisation und Datenverarbeitung des Bischöflichen Ordinariates Augsburg
- in Ausnahmefällen die örtliche Kirchenstiftung für deren APC's ohne Terminalanbindung

Als ***Diözesennetz*** im Sinne dieser Richtlinie gilt die gemeinsame, solidarische, interne Kommunikationsinfrastruktur, welche in einem geschlossenen und nach außen abgesicherten Intranet mit einer einheitlichen Umgebung eine Verbindung der lokalen Netze der beteiligten (Erz-)Diözesen gewährleistet.

Das Diözesennetz entstand aus der Interessengemeinschaft der Bayerischen Diözesen (Arbeitsgemeinschaft Netz) im Jahr 2000. Im Juli 2000 wurde das Bayerische Diözesennetz gegründet.

3. Geltungsbereich

Diese Richtlinie gilt für alle Mitarbeiterinnen und Mitarbeiter sowie für ehrenamtlich Tätige in der Diözese Augsburg, die APC's im Sinne dieser Richtlinie benutzen.

Ausgenommen hiervon sind APC's

- des Caritasverbandes für die Diözese Augsburg e.V.
- der Katholische Jugendfürsorge der Diözese Augsburg e.V.

4. Nutzungszweck

APC dienen den Benutzern ausschließlich zur Erfüllung der dienstlichen/ehrenamtlichen Aufgaben; sie dürfen deshalb nur für diese Zwecke genutzt werden.

4.1 Verbot der anderweitigen Nutzung

Anderweitige Nutzungen, insbesondere folgende, sind untersagt:

- Anschluss nicht dienstlicher Datenverarbeitungssysteme oder von deren Teilkomponenten (Hardware) an dienstliche Systeme (siehe Nr. 2 Begriffsbestimmung)
- Übertragen von Software und Dateien auf Datenträger und andere Datenverarbeitungssysteme (z.B. Laptop, Smartphone, u. ä.) für die Nutzung außerhalb des übertragenen Aufgabenbereiches (z.B. Privatnutzung, Nebentätigkeit u.ä.)
- private Software (z.B. Spiele, Demos, Zeitschriften-CD-ROM´s, Hilfsprogramme, Einkommensteuerprogramme, Bildschirmschoner, Hintergrundbilder, u.ä.) auf dem APC zu installieren und zu betreiben
- Einsatz von Shareware-Software
- private Dateien, Datenbanken etc. im Arbeitsspeicher oder auf der Festplatte einzurichten (siehe auch Nr. 5.2)
- Software, Daten, Internet, E-Mail usw. für private Zwecke zu verwenden, sowie betriebsfremden Personen oder Institutionen für deren Zwecke zur Verfügung zu stellen oder in sonstiger Weise zugänglich zu machen. § 2 Teil. D, 2. ABD bleibt unberührt.

4.2 Ausnahmen der anderweitigen Nutzung

Ausnahmen hiervon sind

- Hardware-Komponenten, die weder einer Installation noch einem Öffnen des APC's bedürfen (z.B. Drucker, Maus, Tastatur, USB-Sticks, Digitalkameras etc. ohne Installationsbedarf), sofern sie nicht anderweitig verboten sind.
- die Nutzung nicht dienstlicher (privater) Datenverarbeitungssysteme zur Nutzung von „CAG" (= Terminalanbindung über DSL- Fremdprovider) und „DME" (= mobiler Outlook-Zugriff mittels Smartphone). Hierbei sind die Vorschriften der Nr. 11 sowie Anlage 3 bzw. Anlage 4 dieser Richtlinie zu beachten.
- dienstlich begründete Ausnahmefälle. Diese bedürfen einer einzelvertraglichen Regelung.

4.3 Nutzung nicht dienstlicher Datenverarbeitungssysteme

Bei sonstiger Nutzung nicht dienstlicher (privater) Datenverarbeitungssysteme im Rahmen des übertragenen Aufgabenbereiches sind insbesondere die in §§ 5b, 6 KDO nebst Anlage zu § 6 KDO enthaltenen Vorschriften einzuhalten.

4.4 Mobile Geräte

Es lässt sich ein deutlicher Trend hin zu mobilen Rechnern (z.B. Notebooks, PDAs, Smartphone etc.) und sonstigen mobilen Geräten (z.B. USB-Stick, externe Festplatten etc.) erkennen. Dabei sind zunächst die gleichen Gefährdungen wie beim Einsatz von „normalen“ APC’s abzusichern.

Zusätzliche Gefahren entstehen beim mobilen Einsatz durch Diebstahl und unbeabsichtigten Verlust. Während in herkömmlicher Büroumgebung der Zugang zu den Geräten abgesichert werden kann, verlassen beim mobilen Einsatz sowohl die Daten als auch das Gerät den Kontrollbereich.

Die organisatorischen und technischen Maßnahmen sind in Abhängigkeit der Sensibilität der personenbezogenen Daten zu wählen; u.a.

- Der Einsatz von mobilen Geräten ist auf das unabweisbar, dienstlich Notwendige zu beschränken.
- Mobile Geräte sind sowohl an der Arbeitsstätte als auch auf Reisen sicher verschlossen aufzubewahren.
- Mobile Geräte sind grundsätzlich für den Bootvorgang seitens DVD-Laufwerke, USB-Sticks und Netzwerke zu sperren, um das Laden eines anderen Betriebssystems unter Umgehung der Sicherungseinstellungen zu verhindern.
- Für die berechtigten Benutzer sind individuelle Kennungen mit individuellen Passwörtern einzurichten.
- Werden bei unabweisbarer, dienstlicher Notwendigkeit sensitive Daten (oder solche, die einem besonderen Berufs- oder Amtsgeheimnis unterliegen) auf mobilen Geräten gespeichert, sind diese Daten mittels einer geeigneten Softwarelösung verschlüsselt zu speichern. Damit soll erreicht werden, dass im Falle eines Diebstahls oder Verlustes des Gerätes die Daten für Dritte nicht verwertbar sind.
- Personenbezogene Daten mit hohem Schutzbedarf (z.B. MW+, adebisKiTa) dürfen nicht auf mobilen Geräten gespeichert, verarbeitet und genutzt werden.

Insbesondere sind die in § 6 KDO nebst KDO-DVO IV. Anlage zu § 6 KDO sowie in Bereichen der freien Jugendhilfe (z.B. Kindertagesstätten) § 78a SGB X und Anlage zu § 78a SGB X enthaltenen Vorschriften einzuhalten.

Alternativ zum Einsatz mobiler Geräte wird die Nutzung von „CAG“ (= Terminalanbindung über DSL-Fremdprovider) und „DME“ (= mobiler Outlook-Zugriff

mittels Smartphone) empfohlen, da hierbei die Daten im Rechenzentrum verarbeitet/gespeichert werden und entsprechend geschützt sind.

Hierbei sind die Vorschriften der Nr. 11 sowie Anlage 3 bzw. Anlage 4 dieser Richtlinie zu beachten.

5. Software

5.1 Einsatz von Software

Auf APC's dürfen nur Originalversionen von Software im Rahmen der Lizenzbedingungen des Herstellers eingesetzt werden.

Die Anfertigung von Softwarekopien zum Zwecke der Weitergabe an andere Dienststellen und Einrichtungen sowie zum Einsatz auf privaten PC's ist aus urheberrechtlichen und strafrechtlichen Gründen strengstens untersagt (Raubkopieren).

5.2 Erstellung von Software etc.

Das Erstellen von Software, Anwendungen, ausführbaren Dateien, sowie Datenbanken (z.B. Access), Plugins, Scripte und Makros (z.B. Microsoft Office) ist auf dienstlichen APC's nur nach schriftlicher Freigabe / Zustimmung der Betreuungseinheit gestattet.

6. Veränderungen am APC und den dazugehörenden Komponenten

Veränderungen an der Hardware des APC's, sowie an sonstigen EDV-Systemen (z.B. PC-Verkabelung, Datendosen, etc.) und an Programmdateien (Software) auf einem APC, sowie Downloads von Software aus dem Internet o.ä. dürfen ausschließlich von der Betreuungseinheit vorgenommen oder beauftragt werden.

7. Wartungs- und Reparaturarbeiten

Wartungs- und Reparaturarbeiten sind ausschließlich von der Betreuungseinheit durchzuführen bzw. von dieser zu beauftragen.

Sofern externe Firmen mit Wartungs-/Reparaturarbeiten beauftragt werden, ist von diesen die Vertraulichkeitserklärung gemäß Anhang 5 zu unterzeichnen.

7.1 Fernwartung

Eine Fernwartung von APC's durch betriebsfremde Firmen birgt besondere Gefahren hinsichtlich der Ausspähung von Daten und ist daher grundsätzlich untersagt.

Ausnahmen können von der Abteilung Organisation und Datenverarbeitung des Bischöflichen Ordinariates freigegeben werden, wenn eine entsprechende Sicherheit gewährleistet werden kann.

8. Wahrung fremder Urheberrechte

Software und Dateien (z.B. Fotos, Kartenmaterial, Schriftfonds, Cliparts, Vorlagen usw.) und zugehörige Handbücher sind in der Regel urheberrechtlich geschützt.

Bei der Nutzung und Weitergabe sind deshalb die geltenden Bestimmungen über die Lizenzierung zu beachten.

9. Zugriffssicherung

APC's und Daten sind vor unberechtigtem Zugriff bzw. unberechtigter Einsichtnahme zu schützen. Hierzu sind auf Systemebene passwortgeschützte Zugriffskontrollen (Benutzername/Passwort) einzurichten.

Im Mehrbenutzer- und Netzwerkbetrieb müssen abgestufte Rechte für den Zugriff auf Software und Daten vergeben werden. Die Einrichtung dieser Zugriffskontrollen sowie die Rechteverwaltung erfolgen durch die Betreuungseinheit.

9.1 Datenablage und Rechteverwaltung

Die Datenablage und Rechteverwaltung ist so zu organisieren, dass Unbefugte keinen Zugriff auf entsprechende Software bzw. Daten erhalten.

Des Weiteren sind die Datenablage und die Rechteverwaltung so zu organisieren, dass im Falle der Abwesenheit (z.B. Krankheitsfall, Urlaub, Sonderurlaub, Elternzeit, Ausscheiden usw.) der Zugriff auf Daten/Dateien und somit ein reibungsloser Arbeitsablauf gewährleistet ist.

9.2 Beantragung/Abmeldung

Die Beantragung erfolgt grundsätzlich über den jeweiligen Stellenleiter (mit Unterschrift) bei der Betreuungseinheit.

Des Weiteren ist die Betreuungseinheit vom jeweiligen Stellenleiter frühzeitig über die Beendigung des Zugriffes (z.B. durch Beendigung des Arbeitsverhältnisses des Mitarbeiters/der Mitarbeiterin usw.) zu informieren.

Hierzu stehen im Intranetportal der Diözese Augsburg entsprechende Anträge zur Verfügung (Applikation „Dokumente“ unter

„EDV/Datenschutz“ → „Formulare/Anträge“).

9.3 Vertraulichkeit der Passwörter

Passwörter sind streng vertraulich zu behandeln und dürfen nicht an Dritte (z.B. Kollegen, unberechtigte Dritte usw.) weitergegeben werden.

Die Verwahrung der Passwörter und Zugangsdaten muss entsprechend sichergestellt werden (z.B. verschlossener Umschlag im Tresor etc.).

Die dienstlich verwendeten Passwörter dürfen nicht auch für private Zwecke / Zugänge genutzt werden (z.B. Zugang zu Social Media oder Online Shops).

9.4 Passwortkomplexität

Passwörter sollten folgende Mindestanforderungen erfüllen:

- mindestens 8 Zeichen lang

- Verwendung von Groß- und Kleinbuchstaben
- Verwendung von Sonderzeichen
- Verwendung von Ziffern

Beispiel für die Bildung eines individuellen, sichern und merkbaren Passwortes:

- PuMhiJ1999g! = **P**aul **u**nd **M**aria **h**aben **i**m **J**anuar **1999 g**eheiratet**!** oder:
- uVWhwiM2006g? = **u**nseren **VW** haben **w**ir **i**m **M**ai **2006 g**ekauft**?**

9.5 Sperrung / Beendigung bei Verlassen des Arbeitsplatzes

Bei Verlassen des Arbeitsplatzes (längere Pausen, Zeiten sonstiger Abwesenheit) ist das laufende Programm vor unberechtigtem Zugriff bzw. unberechtigter Einsichtnahme zu schützen/sperren (z.B. bei Windows-Systemen die Tastenkombination 🗁 + L oder STRG + ALT

+ ENTF mit Klick auf Schaltfläche „Lock Workstation“ bzw. „Computer sperren“).

Bei Dienstende ist das laufende Programm ordnungsgemäß zu beenden und die Abschaltung des APC’s hat zu erfolgen.

9.6 Rücksetzung von Passwörtern

Die Rücksetzung von Passwörtern erfolgt grundsätzlich durch Beantragung (Formular „GV-DV07“) über den jeweiligen Stellenleiter (mit Unterschrift) oder dessen Stellvertreters bei der Betreuungseinheit.

9.7 Notfallregelung

In Notfällen können auf Anordnung des Ordinarius, des Generalvikars oder des hierzu von ihm Beauftragten Passwörter zurückgesetzt bzw. anderweitige Zugriffsrechte gesetzt werden.

10. Abwehr von Viren und Schadsoftware

Computerviren und andere schädliche Software finden eine immer weitere Verbreitung und verursachen große Schäden und Kosten in den befallenen APC’s oder Netzwerken. Ein Computervirus, der aus Unachtsamkeit auf einen APC eingeschleust wurde, kann sich durch einen Netzwerkverbund im gesamten Netzwerkbereich ausbreiten.

10.1 Virenprüfprogramm (Anti-Viren-Software)

Auf APC’s sind entsprechende Maßnahmen (z.B. mittels eines aktuellen, von der Betreuungseinheit vorgeschriebenen Virenprüfprogramm) zur Abwehr von Viren und Schadsoftware zu treffen; dies betrifft alle eingehenden Programm- und Datenträger (z.B. CD’s, DVD’s, USB-Sticks, externe Festplatten u.a.), gleich welcher Herkunft.

Dieses Virenprüfprogramm ist regelmäßig auf Aktualität zu prüfen und entsprechende Suchläufe sind durchzuführen.

10.2 Virenwarnungen

Bei Virenwarnungen sind ausschließlich die Hinweise der Betreuungseinheit zu befolgen. Mögliche Hinweise Dritter sind zu ignorieren (möglicherweise SPAM).

In Zweifelsfällen ist unverzüglich Rücksprache mit der Betreuungseinheit zu halten.

11. Internet/E-Mail/Datenfernübertragung

An APC's, die mit dem Diözesennetzerbunden sind, dürfen aus Sicherheitsgründen keine sonstigen Geräte zur Fernkommunikation (z.B. Modem, ISDN-Karte, Fax-Karte, WLAN, DLAN, DSL, Smartphone mit bestehender Datenverbindung etc.) angeschlossen werden.

Ausnahmen können ausschließlich von der Abteilung Organisation und Datenverarbeitung des Bischöflichen Ordinariates freigegeben werden, wenn sie eine vergleichbare Sicherheit gewährleisten kann (z.B. Fax-Karte am Druckkopierer Epson WP-4595).

Internetzugänge und E-Mail-Adressen im Diözesennetz werden nur entsprechend der dienstlichen Bedürfnisse nach dem jeweiligen Antragsverfahren der (Erz-)Diözese vergeben.

APC's, die nicht am Diözesennetz, sondern an die eigene Fernkommunikationseinrichtungen angeschlossen sind (z.B. per DSL-Modem, ISDN-Karte, Fax-Karte etc.), sind besonders den Gefahren durch Computerviren und unberechtigtem Zugriff ausgesetzt. Maßnahmen zur Gefahrenabwehr sind gesondert festzulegen.

Verboten ist die Verarbeitung und Speicherung von personenbezogenen Daten und Daten des dienstlichen Gebrauchs (vgl. Nr. 12 Datenschutz) auf diesen APC's.

Im Übrigen bleibt eine gesonderte Regelung zur Nutzung von E-Mail- und Internetdiensten vorbehalten.

12. Datenschutz

Bei der Verarbeitung und Speicherung von personenbezogenen Daten sind die Datenschutzvorschriften gemäß der KDO, der KDO-DVO, der IT-Richtlinie und ggf. weitere bereichsspezifische Normen (z.B. nach den Sozialgesetzbüchern) und Richtlinien in der jeweils geltenden Fassung zu beachten.

Informationen und Daten des dienstlichen Gebrauchs, insbesondere Betriebs- oder Geschäftsgeheimnisse, sowie personenbezogene Daten aller Art, deren Vertraulichkeit oder Geheimhaltungsbedürftigkeit nach gesetzlicher Vorschrift gegeben ist oder die vom Arbeitgeber ausdrücklich als vertraulich oder geheimhaltungsbedürftig bezeichnet werden, sind wenigstens der Datenschutzklasse II (siehe IT-Richtlinie) zugeordnet (= Daten, deren Missbrauch den Betroffenen in

seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigen kann).

Solche personenbezogenen Daten und Daten des dienstlichen Gebrauchs dürfen nicht auf APC's gespeichert werden, die über einen anderen Internetzugang als das Diözesennetz (Ausnahmereglung bei

„CAG" und „DME" – siehe Nr. 11 sowie Anlage 3 bzw. Anlage 4 dieser Richtlinie) verfügen.

13. Datensicherung

Die erfassten und erzeugten Daten haben einen hohen Wert und sind deshalb gegen Verlust zu sichern. Damit bei einem Hard-/ Softwareabsturz wichtige Dateien wieder hergestellt werden können, müssen diese in regelmäßigen, kurzen Abständen (i.d.R. täglich) auf ein entsprechendes Sicherungsmedium kopiert und vor Fremdzugriff, sowie vor Verlust und Zerstörung sicher verwahrt werden.

Für die erforderliche Datensicherung auf den zentralen Servern ist die Betreuungseinheit verantwortlich.

Die Benutzer sind gehalten, alle Daten soweit möglich auf den zentralen Servern abzulegen. Grundsätzlich sind dienststellenbezogene Daten auf den zur Verfügung gestellten Gruppenlaufwerken abzulegen.

Falls Daten direkt auf dem APC (auf der Festplatte) gespeichert werden müssen, ist der Anwender für die erforderliche Sicherung selbst verantwortlich.

Dies trifft auch für die Datensicherung bei nicht vernetzten APC's zu.

14. Außerbetriebnahme von APC's

14.1 Rückgabe und Herausgabe

Der APC einschließlich aller Komponenten, Passwörter und Daten ist mit der Beendigung des Beschäftigungsverhältnisses und jederzeit auf Verlangen des jeweiligen gesetzlichen Vertreters des Rechtsträgers bzw. dessen Beauftragten an diesen herauszugeben.

14.2 Verwertung von APC's

APC's sollten seitens des Eigentümers (i.d.R. die Betreuungseinheit) nicht verkauft werden, da entsprechende Gewährleistungen nicht übernommen werden können.

Eine Verschenkung z.B. für einen karitativen Zweck bzw. eine Verbringung z.B. ins Pfarrheim etc. ist möglich.

Die Festplatten und sonstige Datenträger sind hierbei grundsätzlich auszubauen und entsprechend zu vernichten (vgl. Punkt 14.3).

Diese können auch der Abt. Organisation und Datenverarbeitung zur Vernichtung zugeführt werden (Formular „GV-DV30").

14.3 Vernichtung von EDV-Ausdrucken und Datenträgern

Werden die

- APC's,
- sonstige Systeme (PDAs, MDAs, Drucker/Kopierer mit internen Speicher u.a.) oder
- Datenträger (Disketten, CDs, DVDs, USB-Sticks, Festplatten, u.a.)

aus dem Betrieb genommen (z.B. Verschrottung, Verschenkung, Verbringung), müssen die Speichermedien unwiederbringlich vernichtet bzw. der Betreuungseinheit übergeben werden.

EDV-Ausdrucke mit personenbezogenen Daten sind durch Aktenvernichter (Schredder) oder durch andere geeignete Maßnahmen (z.B. Verbrennen), die die Lesbarkeit oder Wiederherstellbarkeit ausschließen, zu vernichten.

Hierzu kann auch eine qualifizierte/zertifizierte Fremdfirma beauftragt werden.

15. Verantwortlichkeit und Haftung

Die Stellenleiter tragen die Verantwortung für eine den Grundsätzen des Datenschutzes und der Datensicherheit (im Besonderen gemäß KDO, insbesondere SGB VIII und X, IT-Richtlinie und dieser Richtlinie) entsprechende Ausübung der Datenverarbeitung in ihren Dienst- stellen.

Sie haben den Benutzern in ihrer Dienststelle diese Richtlinie und zukünftige Änderungen bekannt zu geben (vgl. Anhang 1) und regelmäßig hierüber aufzuklären.

Die Haftung der Benutzer von APC's bei Verstößen gegen diese Richtlinie richtet sich nach den jeweils geltenden vertraglichen und gesetzlichen Bestimmungen.

16. Schlussbemerkungen

Weitere Hinweise zu den einzelnen Punkten können in der Betreuungseinheit eingeholt werden.

17. Inkrafttreten

Diese Richtlinie tritt am 01.12.2014 in Kraft. Sie ersetzt alle früheren APC-Richtlinien.

Anhang 1 zur APC-Richtlinie

Verpflichtungserklärung für (besoldete) MitarbeiterInnen

Ich (Vor- und Zuname) _____

geboren am _____

wohnhaft in _____

verpflichte mich: _____

- Die Anordnung über den kirchlichen Datenschutz – KDO – in der Diözese Augsburg und die zu ihrer Durchführung ergangenen Bestimmungen in der jeweils geltenden Fassung einzuhalten.
- Die Richtlinie für die Benutzung von Arbeitsplatzcomputern (APC) in der Diözese Augsburg in der jeweils geltenden Fassung einzuhalten.
- Bei Auffälligkeiten, Fehlern oder dem Verdacht von Unregelmäßigkeiten an dem APC oder an Daten sofort die Betreuungseinheit zu benachrichtigen.

Ich bin mir bewusst, dass ein Verstoß gegen diese Bestimmungen arbeits-, zivil- und/oder strafrechtliche Konsequenzen nach sich ziehen kann.

Gleichzeitig bestätige ich durch meine Unterschrift die Aushändigung eines Abdrucks dieser Richtlinien bzw. die Zugangsmöglichkeit (Intranetportal, Amtsblatt etc.) zu haben.

Diese Erklärung wird zu der Personalakte bzw. zu den Unterlagen genommen.

_____ _____

Ort, Datum Unterschrift

Anhang 2 zur APC-Richtlinie

Verpflichtungserklärung für Ehrenamtliche

gemäß § 4 der Anordnung über den kirchlichen Datenschutz - KDO -

Ich (Vor- und Zuname) _____

geboren am _____

wohnhaft in _____

bin bei/in _____

ehrenamtlich tätig und verpflichte mich:

- Die Anordnung über den kirchlichen Datenschutz – KDO – in der Diözese Augsburg und die zu ihrer Durchführung ergangenen Bestimmungen in der jeweils geltenden Fassung einzuhalten und bestätige, dass ich auf die wesentlichen Grundsätze der für meine Tätigkeit geltenden Bestimmungen hingewiesen wurde.
- Daten, die ich aufgrund meines Ehrenamtes erhalten habe oder die mir im Zusammenhang mit meinem Ehrenamt zur Kenntnis gelangt sind, während der Tätigkeit und nach ihrer Beendigung vertraulich zu behandeln.
- Die Richtlinie für die Benutzung von Arbeitsplatzcomputern (APC) in der Diözese Augsburg in der jeweils geltenden Fassung einzuhalten.
- Bei Auffälligkeiten, Fehlern oder dem Verdacht von Unregelmäßigkeiten an dem APC oder an Daten sofort die Betreuungseinheit zu benachrichtigen.

Ich bin mir bewusst, dass ein Verstoß gegen diese Bestimmungen zivil- und/oder strafrechtliche Konsequenzen nach sich ziehen kann.

Gleichzeitig bestätige ich durch meine Unterschrift die Aushändigung eines Abdrucks dieser Richtlinien bzw. die Zugangsmöglichkeit (Intranetportal, Amtsblatt etc.) zu haben.

_____ _____

Ort, Datum Unterschrift

Anhang 3 zur APC-Richtlinie

Zusatz zur Nutzung eines CAG – Zugangs

Ich verpflichte mich:

- Im Zusammenhang mit meiner Arbeit zentrale Software nur an einem PC zu nutzen, der über einen aktuellen Virenscanner (aktuelle Virendefinition) verfügt und mit einer Firewall ausgestattet ist.
- Die Kosten für die Hardware, das Verbrauchsmaterial, sowie für die Datenverbindung privat zu tragen (dienstlich begründete Ausnahmefälle bedürfen einer einzelvertraglichen Regelung).
- Die dienstlichen Daten nur im Bereich des zur Verfügung gestellten CAG-Zugriffes (u.a. AST Desktop) zu nutzen (nur in Ausnahmefällen dürfen Daten auf den privaten PC kopiert werden).
- Erstellte Ausdrucke in einem verschließbaren Schrank oder auf andere Weise vor Zugriffen Dritter zu schützen.
- Die Vorschriften der KDO, der IT-Richtlinien etc. bei allen Arbeiten mit dienstlichen Daten bzw. für dienstliche Stellen zu befolgen.
- Die Richtlinie für die Benutzung von Arbeitsplatzcomputern (APC) in der Diözese Augsburg in der jeweils geltenden Fassung einzuhalten.
- Den Token entsprechend sicher aufzubewahren und vor Fremdzugriff bzw. Missbrauch zu schützen.
- Bei Verlust/Diebstahl des Tokens bzw. des Mobilfunkgerätes (auch bei Kündigung des Mobilfunkvertrages oder Änderung der Rufnummer) die Abteilung Organisation und Datenverarbeitung des Bischöflichen Ordinariates unverzüglich zu informieren.
- Bei Beendigung des Dienstverhältnisses die Abteilung Organisation und Datenverarbeitung des Bischöflichen Ordinariates unverzüglich zu informieren und gegebenenfalls den Token zurückzugeben.

Diese Erklärung wird zu meinen Personalakten genommen.

Name, Vorname in Klarschrift _____

_____ _____

Ort, Datum Unterschrift

Anhang 4 zur APC-Richtlinie

Zusatz zur Nutzung von DME

Ich verpflichte mich:

- Die dienstlichen Daten (E-Mails, Anlagen zu E-Mails, Kontakte, Kalendereinträge etc.) nur in der entsprechenden (Smartphone-)Applikation (App) zu nutzen (Datensicherheit ist nur so gewährleistet).
- Die Vorschriften der KDO, der IT-Richtlinien etc. bei allen Arbeiten mit dienstlichen Daten bzw. für dienstliche Stellen zu befolgen.
- Die Richtlinie für die Benutzung von Arbeitsplatzcomputern (APC) in der Diözese Augsburg in der jeweils geltenden Fassung einzuhalten.
- Die Kosten für das Smartphone bzw. Verbindungsgerät sowie für die Datenverbindung privat zu tragen (Dienstlich begründete Ausnahmefälle bedürfen einer einzelvertraglichen Regelung).
- Bei Verlust/Diebstahl des Smartphones bzw. des Verbindungsgerätes (auch bei Kündigung des Mobilfunkvertrages oder Änderung der Rufnummer) die Abteilung Organisation und Datenverarbeitung des Bischöflichen Ordinariates unverzüglich zu informieren.
- Bei Beendigung des Dienstverhältnisses die Applikation, sowie alle dienstlichen Daten auf dem Smartphone bzw. dem Verbindungsgerät zu löschen.

Diese Erklärung wird zu meinen Personalakten genommen.

Name, Vorname in Klarschrift _____

_____ _____

Ort, Datum Unterschrift

Anhang 5 zur APC-Richtlinie

Vertraulichkeitserklärung wegen durchzuführender Installations-/Wartungs-/Reparaturarbeiten an Arbeitsplatzcomputern (APC)/Servern

Diese Vertraulichkeitserklärung wird wegen durchzuführender Installations-/Wartungs-/Reparaturarbeiten an Arbeitsplatzcomputern (APC)/Servern

☐ des Bischöflichen Ordinariates Augsburg

☐ der Kath. Pfarrkirchenstiftung _____ in _____

☐ der sonstigen kirchlichen Stelle _____

abgegeben.

Herr/Frau/Firma _____
(nachgenannt Auftragnehmer)

sichert zu, dass alle im APC/Server enthaltenen oder über eine Vernetzung zugänglichen Daten vertraulich behandelt und nicht an Dritte weitergegeben werden.

Der Auftragnehmer haftet für alle aus der Verletzung dieser Zusicherung dem Auftraggeber entstehenden Schäden und stellt insofern den Auftraggeber von allen Schadensansprüchen Dritter frei.

_____	_____
Ort, Datum	Unterschrift Auftragnehmer
_____	_____
Ort, Datum	Unterschrift Auftraggeber