ABl 13/2020, S. 456-467

Benutzerrichtlinie zur Informationssicherheit

1 Einleitung

Die Abhängigkeit von modernen Informations- und Kommunikationstechnologien bei der Verarbeitung von Informationen nimmt immer weiter zu, genauso wie die fortschreitende Vernetzung sowohl der Diözese Augsburg, als auch ihrer Beschäftigten - im beruflichen wie im privaten Bereich - mit anderen Diözesen, Behörden und Personen durch eine immer intensivere Nutzung sozialer Medien und Netzwerke.

Die verarbeiteten Daten reichen dabei von personenbezogenen Daten der Gläubigen und Mitgliedern der Diözese bis hin zu vertraulichen Finanzdaten und anderen sensiblen und damit schützenswerten Daten.

Die Einhaltung der Informationssicherheit ist damit einhergehend unverzichtbar. Informationen und Daten müssen bestmöglich hinsichtlich ihrer Vertraulichkeit, Integrität und Verfügbarkeit geschützt werden.

Diese Richtlinie beschreibt die Mindestanforderungen der Informationssicherheit bei der Arbeit und dem Umgang mit IT-Systemen in der

täglichen Praxis. Weiterhin werden die grundlegenden Verhaltensregeln zur Informationssicherheit beschrieben. Weitere detaillierte Regelungen über diese Grundlagen hinaus finden Sie in den entsprechenden Informationssicherheitsrichtlinien.

Die nachfolgenden Regeln sind für die Diözese Augsburg und die unter ihrer Aufsicht stehenden Rechtsträger von großer Bedeutung und daher verpflichtend anzuwenden.

Informationssicherheit liegt in der Verantwortung jedes Einzelnen.

2 Geltungsbereich

Diese Richtlinie gilt für das Bischöfliche Ordinariat des Bistum Augsburg und die der Aufsicht der Diözese unterstehenden Rechtsträger.

3 Begriffsklärungen

Benutzer Benutzer im Sinne dieser Richtlinie sind alle Mitarbeitenden (Beschäftigte, Ehrenamtliche, externe Dienstleister), die Zugriff auf Informationen und informationsverarbeitende Einrichtungen der Diözese Augsburg erhalten.

IKT Informations- und Kommunikationstechnologie. Hiermit sind alle technischen Geräte wie z.B. PCs, Workstations, Laptops, Tablets, Smartphones, Telefone usw. eingeschlossen

4 Allgemeine Regelungen

Die Diözese Augsburg stellt den Benutzern eine leistungsfähige IKT- Infrastruktur als Arbeitsmittel im Rahmen der Aufgabenerfüllung zur Verfügung. Diese dient insbesondere der Erleichterung der internen und externen Kommunikation, der Erzielung einer höheren Effizienz und der Beschleunigung der Informationsbeschaffung und der Arbeitsprozesse.

Hierbei gelten folgende grundsätzliche Regelungen:

- Die zur Verfügung gestellten Betriebsmittel, Ausstattungen und Dokumentationen sind pfleglich zu behandeln.

- Eine Weitergabe von Informationen und Ausstattungen an unbefugte Dritte ist nicht erlaubt.
- Ein Verlust oder Beschädigung muss unverzüglich an den Vorgesetzten und die Stabsabteilung IT und Digitalisierung des Generalvikars gemeldet werden.
- In allen Räumen müssen die Türen und Fenster bei längerem Verlassen des Arbeitsplatzes oder Beendigung der Arbeit geschlossen werden, um Einbruch und Entwenden von Informationen und Betriebsmitteln zu verhindern.
- In Räumen mit Publikumsverkehr müssen Bildschirme so aufgestellt werden, dass Dritte keine Sicht auf den Bildschirm erhalten.
- Konfigurations- und insbesondere Sicherheitseinstellungen an Hard- und Software dürfen durch Benutzer nicht verändert werden. Einstellungsänderungen können bei der Stabsabteilung IT und Digitalisierung des Generalvikars über die bekannten Prozesse beantragt werden.
- Die Anfertigung von Softwarekopien zum Zwecke der Weitergabe an andere Dienststellen und Einrichtungen sowie zum Einsatz auf privaten PCs ist untersagt, sofern dieses der Urheber nicht ausdrücklich erlaubt.
- Die Installation von Software bzw. Applikationen jeder Art auf dienstlich zur Verfügung gestellten IT Geräten seitens der Benutzer ist strengstens untersagt. Das gilt auch für portable Anwendungen, die keine Installation erfordern.

  Falls zusätzliche, nicht im Standard der IT enthaltene Software benötigt wird, kann diese in der Stabsabteilung IT und Digitalisierung des Generalvikars über die bekanntgegebenen Prozesse jederzeit beantragt werden.

5 Aufgeräumter Arbeitsplatz

Unter einem aufgeräumten Arbeitsplatz (Clear Desk) versteht man, dass Mitarbeiter alle vertrauliche Dokumente, die sich auf ihrem Arbeitsplatz befinden, nach Arbeitsschluss oder bei Verlassen des Arbeitsplatzes verschließen. Unbefugte Personen dürfen keinen Zugriff darauf erhalten.

Im Besonderen ist zu beachten:

- Bei Verlassen des Arbeitsplatzes müssen alle sensiblen Ausdrucke, Dokumente, Akten, Datenträger usw. so verstaut werden, dass diese Dokumente nicht für Dritte zugänglich sind. Türen, Schreibtische und Sideboards sind abzuschließen.
- Lassen Sie bitte keine Ausdrucke im Drucker/Kopierer liegen.
- Bewahren Sie unter keinen Umständen Passwortnotizen an ihrem Arbeitsplatz auf.
- Sperren Sie ihren Computer, wenn Sie ihren Arbeitsplatz verlassen (z. B. unter Windows mit „Windows-Taste + L“). Unbeaufsichtigte, nicht gesperrte Computer sind ein hohes Sicherheitsrisiko, denn Unbefugte können so leicht Zugang zu vertraulichen Daten erhalten.

6 Urheberrechte

Fotos, Kartenmaterial, Schriften, Clip Arts, Vorlagen usw. sind oft urheberrechtlich geschützt. Die Benutzer sind selbst verantwortlich, die Lizenzbestimmungen zu klären und Urheberrechtsverletzungen zu vermeiden.

7 E-Mails, Spam und Schadsoftware

E-Mail gehört zum Standard in der beruflichen Kommunikation. Cyberkriminelle versenden daher immer wieder E-Mails mit schadhaften Links oder virenbehafteten

Dokumenten im Anhang (z.B. Excel, Word, PDF). Oft geht es darin um vermeintliche Probleme mit Rechnungen, das Sperren von Zugängen oder die Bitte um Aktualisierung von persönlichen (Zugangs-)Daten. Unsere Sicherheitssysteme erkennen solche Angriffe mit hoher Wahrscheinlichkeit. Dennoch kann es vorkommen, dass Sie eine solche E-Mail erhalten.

Bei der Nutzung des dienstlichen E-Mail Accounts ist daher zwingend zu beachten:

- Bitte seien Sie besonders kritisch bei E-Mails von unbekannten Absendern, insbesondere mit Links oder Dateianhängen. Wenn ihnen Absender oder Betreffzeile verdächtig erscheinen, öffnen sie die E-Mail nicht.
- Achten Sie auf die Formulierungen im Anschreiben – entsprechen sie den Gepflogenheiten einer guten geschäftlichen Kommunikation?
- Vorsicht aber auch bei bekannten Absendern. E-Mailadressen sind leicht zu fälschen und werden zunehmend für Cyberkriminalität genutzt. Fragen Sie sich: Ist die E-Mail der Person zu diesem Anlass nachvollziehbar? Passt der Text der E-Mail zum Absender? Erwarten Sie die beigelegten Dateien und passen sie zum Absender, oder kommen sie völlig unerwartet?
- Kreditinstitute und seriöse Firmen fordern niemals per Telefon oder per E-Mail und Links zur Übermittlung von Zugangsdaten wie beispielsweise Online-Banking-Daten oder Passwörtern (z.B. PIN oder TAN) auf. Die angeforderten, vertraulichen Informationen dürfen Sie auf keinen Fall weitergeben.
- Antworten Sie nicht auf verdächtige E-Mails. Die Rückmeldung bestätigt dem Spam-Versender lediglich die Gültigkeit ihrer Mail-Adresse und erhöht dadurch das Risiko, weitere Zusendungen zu erhalten.

Die wichtigste Regel lautet: Im Zweifelsfall keine Anhänge öffnen,
nicht auf Links klicken und die E-Mail löschen.

Der Cyberkriminelle meldet sich nicht wieder. War die E-Mail aber berechtigt und wichtig, so wird sich der Geschäftspartner oder Kollege*in noch einmal an Sie wenden. Ein Telefonanruf kann hier ebenfalls klärend sein, denn Cyberkriminelle arbeiten nicht mit echten Telefonnummern.

Bei individuellen Fragen unterstützt Sie dabei auch der Leiter der Stabsstelle Informationssicherheit.

8 Dienstliche und private Nutzung von Hard- und Software

Private Nutzung

Dienstlich zur Verfügung gestellte IKT, egal ob ortsgebunden oder mobil, dürfen grundsätzlich nicht zu privaten Zwecken verwendet werden. Das betrifft auch die Verwendung des dienstlichen E-Mail-Accounts und die Nutzung von Internet-Diensten. Hier sind im Besonderen die Regelungen der ABD Teil D, 2 „Regelung zur Kontrolle der Nutzungsbeschränkung von Internet-Diensten“ zwingend zu beachten.

Dienstliche Nutzung

Die Nutzung privater Geräte zur dienstlichen Zwecken ist grundsätzlich unzulässig.

Private Hard- und Software und elektrische Geräte sowie private Internet- und E-Mail-Accounts dürfen nicht für geschäftliche Zwecke genutzt werden. Private elektrische Geräte dürfen nicht an die gestellten Betriebsmittel oder das Netzwerk angeschlossen werden. Dazu gehören auch private mobile Datenträger aller Art.

Private Smartphones dürfen lediglich eng begrenzt unter Einsatz einer sicheren Containerlösung, die den Benutzern ausschließlich über die Stabsabteilung IT und

Digitalisierung des Generalvikars zur Verfügung gestellt wird, für die dienstliche Kommunikation verwendet werden.

Ausnahmen für besondere Nutzergruppen (Ehrenamtliche, Religionslehrer etc.) sind in den „erläuternden Hinweisen zur Durchführungsverordnung zum Gesetz über den kirchlichen Datenschutz“ (Amtsblatt Nr. 6 vom 18. April 2019, Seite 237 ff.) geregelt.

9 Dienstliche Nutzung des Internets

Mitarbeiter sind zu einer verantwortungsbewussten und produktiven Internetnutzung angehalten. Der Internet-Zugang ist nur für Aktivitäten im Rahmen der ausgeübten beruflichen Tätigkeit vorgesehen und darf nicht für persönliche Zwecke verwendet werden. Auch bei dienstlich veranlasster Nutzung von Internet-Diensten, z.B. zu Recherchezwecken, bestehen Risiken. Es liegt in persönlicher Verantwortung der Nutzer, solche Bedrohungen durch entsprechendes Verhalten zu vermeiden oder zu erkennen und entsprechend darauf zu reagieren.

Die nicht akzeptable Nutzung des Internets durch Mitarbeiter umfasst u. a. folgende Aktivitäten, die untersagt sind:

- Übermittlung bzw. Veröffentlichung von diskriminierenden, belästigenden oder bedrohenden Mitteilungen oder Bildern über den E-Mail-Dienst des Bistums Augsburg bzw. im Internet.
- Aufruf von Websites mit pornografischen, gewaltverherrlichenden, strafrechtlich bedenklichen oder kirchenfeindlichen Inhalten. Das kann gravierende rechtliche Konsequenzen – auch für die Diözese – nach sich ziehen.
- Besuch von Seiten, die einen illegalen Hintergrund vermuten lassen wie beispielsweise Seiten mit Raubkopien oder anderen urheberrechtlich verletzten Inhalten.
- Missbrauch von Computern für Betrugszwecke und/oder für Software-, Film- und Musik-Raubkopien.
- Herunterladen und Kopieren von urheberrechtlich geschützter Software und elektronischen Dateien ohne ausdrückliche Genehmigung, das Erstellen von Raubkopien eingeschlossen.
- Übermittlung bzw. Veröffentlichung von Informationen, die für das Bistum, seine Mitarbeiter und die Gläubigen rufschädigend sein können.
- Übermittlung bzw. Veröffentlichung von Kettenbriefen und Werbung, die nicht im Interesse interner Geschäftsaktivitäten stehen.
- Äußerung eigener, persönlicher Meinungen unter dem Namen des Bistums.

10 Passwörter

Passwörter für den Zugang zum diözesanen Netzwerk, zum E-MailAccount oder zu Fachanwendungen sind wie Haustürschlüssel für das eigene Zuhause: Nur ein sicheres Passwort schützt vor ungebetenen Gästen und deren Zugriff auf Informationen, egal ob beruflich oder privat.

Dabei gilt für den virtuellen Schlüssel wie für den Haustürschlüssel: je komplexer er ist, umso schwieriger ist er zu knacken. Im Besonderen beim sog. „Single Sign On“ (einmalige Anmeldung, Zugang zu allen Anwendungen), wie es im Netzwerk der Diözese Augsburg üblich ist, muss ein starkes Passwort verwendet werden.

Passwörter müssen mindestens 8 Zeichen lang sein. Ein Passwort muss wenigsten 3 der folgenden 4 Kriterien einhalten, sofern dieses technisch umsetzbar ist:

- Großbuchstaben
- Kleinbuchstaben
- Ziffer

- Sonderzeichen

Beim Umgang mit Passworten sind die folgenden Regeln einzuhalten:

- Niemals den eigenen Namen, Vornamen, Geburtsdaten, Durchwahlen, etc. oder solche Daten von Familienmitgliedern, Freunden oder Bekannten verwenden. Diese werden bei Angriffen zuerst ausprobiert.
- Verwenden Sie keine Begriffe aus einem Wörterbuch (auch nicht in einer anderen Sprache). Es gibt Schadsoftware, die Wortlisten abruft und so mögliche Passwörter findet. Auch Eigennamen, geografische Begriffe etc. dürfen nicht verwendet werden.
- Trivialpasswörter (hallohallo, abcdefgh, 08/15, 12345678, qwertzui, passwort etc.) sind ebenfalls unzulässig. Sie können von anderen leicht beim Beobachten der Passworteingabe erkannt werden und werden in Sekunden geknackt.
- **Passwörter sind geheim zu halten.** Bei der Eingabe ist darauf zu achten, dass sie nicht von Dritten eingesehen werden können.
- Geben Sie ihr Passwort an niemanden, auch nicht an Vorgesetzte, weiter.
- Jeder Nutzer benötigt ein eigenes Passwort, das gilt auch für Auszubildende, Praktikanten, Ehrenamtliche etc.
- Der Gebrauch von anonymen Kennungen, mit denen mehrere Mitarbeiter arbeiten, ist untersagt. Ausnahmen müssen durch den Leiter der Stabsstelle Informationssicherheit genehmigt werden.
- Passwörter dürfen nicht unverschlüsselt in Dateien abgelegt werden.
- Ersetzen Sie voreingestellte Passwörter (Initialpasswörter) umgehend bei der ersten Anmeldung durch ein persönliches Passwort.
- Notieren Sie keine Passwörter im Klartext ungeschützt in der Nähe ihres Arbeitsplatzes.
- Passwörter sind unverzüglich zu wechseln, wenn der Verdacht besteht, dass sie Dritten bekannt geworden sein könnten.
- Verwenden Sie Passwörter, die Sie im privaten Umfeld nutzen, nicht im beruflichen Bereich. Trennen Sie strikt private und geschäftliche Passwörter.
- Passwörter dürfen nicht als Teil eines automatischen Anmeldeprozesses verwendet werden, z.B. in einer Funktionstaste oder im Passwort-Tresor eines Internet-Browsers.

11 Datenspeicherort und Datensicherung

Die Dateien, die während der Arbeit am PC, Laptop oder anderen mobilen Geräten erstellt werden, sind auf den Netzwerklaufwerken (Laufwerke T:\, U:\ usw.) zu speichern. Alle Dateien auf den Netzlaufwerken werden automatisch von der Datensicherung erfasst.

Falls Daten kurzfristig lokal auf dem Gerät gespeichert werden (Laufwerk C:\), z.B. wenn kein Zugriff zum Netzwerk besteht, müssen diese bei der nächsten Anmeldung im diözesanen Netzwerk auf dem Fileserver abgelegt werden. Der Benutzer hat damit die Verantwortung, dass die von ihm lokal abgelegten Dateien durch Ablage auf den Netzlaufwerken mit in der Datensicherung gesichert werden können.

12 Löschen von Informationen und Datenträgern

Im Papierkorb am Arbeitsplatz entsorgte Dokumente und Datenträger mit sensiblen Informationen stellen ein ernstes Sicherheitsrisiko dar, wenn diese Daten in falsche Hände geraten. Aus diesem Grund müssen Dokumente und Datenträger (USB Stick, Festplatte, SD Karten, CD/DVD…) sicher entsorgt werden.

Bei der Entsorgung von Dokumenten und Datenträgern ist zwingend zu beachten:

- Datenträger oder sensible Dokumente dürfen auf keinen Fall in den Papierkorb geworfen werden.
- Sensible Dokumente müssen per Aktenvernichter (Schredder) oder in einer abgeschlossenen Datenschutztonne entsorgt werden.
- Datenträger, die entsorgt werden sollen, müssen an die IT- Abteilung übergeben werden. Die Geräte werden durch die IT- Abteilung fachgerecht entsorgt.
- In jeder Organisationseinheit ist eine Person zu benennen, die für die sichere Entsorgung zuständig ist.
- Für alle Fälle von Aussonderungen oder Vernichtung von Schriftgut und Datenträgern gelten die Maßgaben der „Durchführungsverordnung für die Anordnung zur Sicherung und Nutzung der Archive der Kath. Kirche (KAO-DVO, Amtsblatt Nr. 6 vom 18. April 2019, Seite 242 ff.) in ihrer jeweils gültigen Fassung.

13 Umgang mit mobilen Endgeräten

Mobile Endgeräte (Laptops, Smartphones, Tablets, Microsoft Surfaces etc.) stellen wegen ihrer ortsungebundenen Verwendungsmöglichkeiten und Attraktivität für Diebe ein erhöhtes Sicherheitsrisiko dar. Die folgenden Verhaltensregeln helfen, wesentliche Risiken zu vermeiden.

Bei der Verwendung mobiler Geräte ist zwingend zu beachten:

- Mobile Geräte sind bei ihrem Transport so zu verwahren, dass sie von Dritten nicht gesehen werden können (z.B. im Kofferraum des KFZ).
- In Hotels müssen die Geräte im Zimmertresor verwahrt werden, wenn ein solcher vorhanden ist.
- Das Gerät darf nicht unbeaufsichtigt gelassen werden.
- Überlassen Sie das Gerät nicht anderen, insbesondere betriebsfremden Personen.
- Achten Sie bei der Passworteingabe in öffentlichen Bereichen darauf, dass Sie während der Eingabe unbeobachtet sind.
- Sofern Sie häufig in öffentlichen Bereichen mit dem Gerät arbeiten, verwenden Sie eine Sichtschutzfolie für das Display des mobilen Geräts. Für weitere Informationen wenden Sie sich bitte an die Stabsabteilung IT und Digitalisierung.
- Melden Sie einen Diebstahl oder Verlust unverzüglich ihrem unmittelbaren Vorgesetzten und der Stabsabteilung IT und Digitalisierung des Generalvikars.

14 Anwendungen und Speicher in der Cloud

Es steht eine Vielzahl von Anwendungen und Datenspeichern in der Cloud zur Verfügung. Dazu gehören

- Office-Programme
- Videokonferenzsysteme
- Datenspeicher
- E-Mailsysteme
- Kalenderfunktionen

und vieles andere mehr.

Es dürfen ausschließlich die von der Stabsabteilung IT und Digitalisierung des Generalvikars zur Benutzung freigegeben Cloud-Dienste verwendet werden. Diese Lösungen sind auch durch den Leiter der Stabsstelle Informationssicherheit und den Datenschutzbeauftragten überprüft worden und aus rechtlicher Sicht vertretbar.

15 Verhalten bei Social Engineering

Unter Social Engineering versteht man den Versuch, Personen zu manipulieren, um Zugang zu vertraulichen Informationen zu erlangen. Überwiegend wird ein solcher Angriff per Telefon oder per E-Mail durchgeführt. Jedoch ist es auch möglich, dass es im persönlichen Kontakt versucht wird. Social Engineering nutzt auf der psychologischen Ebene grundlegende menschliche Eigenheiten aus. Das Erwerben oder Erschleichen von Vertrauen nimmt hierbei eine zentrale Rolle ein. Um dieses Vertrauen aufzubauen, müssen Angreifer eine weitreichende Kenntnis der Zielorganisation oder -person haben. Das bedeutet, dass im Vorfeld eine umfangreiche Informationssammlung stattgefunden hat.

Social Engineers geben sich gerne als Mitarbeiterinnen oder Mitarbeiter aus oder behaupten, eine Behörde oder ein wichtiges Kundenunternehmen zu vertreten. Die Opfer werden durch firmeninternes Wissen oder Kenntnisse spezieller Fachbegriffe getäuscht, die sie sich

zuvor durch Telefonate oder Gespräche mit anderen Kollegen erworben haben. Beim Angriff appellieren sie dann an Ihre Hilfsbereitschaft oder drohen als „Kunde“ mit massiven Beschwerden bei Vorgesetzten oder der Diözesanleitung.

Bitte beachten Sie daher unbedingt folgende Punkte:

- Seien Sie bei Telefonanrufen oder E-Mails skeptisch, besonders wenn der Auftrag oder die Bitte des Kollegen, “in dessen Auftrag” eine Anfrage gestellt wird, sehr ungewöhnlich ist.
- Bitten Sie darum, denjenigen zurückzurufen. Kriminelle sind nicht daran interessiert, Telefonnummern etc. preiszugeben.
- Falls möglich, besprechen Sie die Angelegenheit mit dem be treffenden Kollegen persönlich.
- Geben Sie niemals vertrauliche Informationen per Telefon oder E-Mail an Dritte weiter, ohne dass mit dieser Partei eine Vertraulichkeitsvereinbarung unterzeichnet wurde.

16 Rückgabe von Betriebsmitteln

Der Benutzer hat die Verpflichtung alle ihm durch den Arbeitgeber zur Verfügung gestellten Betriebsmittel bei Beendigung des Arbeitsverhältnisses oder des Vertrages zurückzugeben. Dieses kann auch beim Wechsel der Arbeitsstelle innerhalb der Diözese notwendig sein.

17 Informationssicherheitsvorfälle

Sobald ein Sicherheitsereignis vermutet wird oder ein Sicherheitsvorfall eingetreten ist, müssen Maßnahmen zur Behebung durchgeführt werden. Hierzu muss unverzüglich eine Meldung an den Leiter der Stabsstelle Informationssicherheit erfolgen.

Kontaktdaten:
E-Mail: informationssicherheit@bistum-augsburg.de
Telefon: 0821/3166-8888

18 Verantwortlichkeiten, Verstöße und Haftung

Die Dienstellenleiter tragen die Verantwortung für eine den Grundsätzen der Informationssicherheit und des Datenschutzes entsprechende Ausübung der Informationsverarbeitung in ihren Dienststellen. Sie haben den Benutzern in ihrer Dienststelle diese Richtlinie und zukünftige Änderungen bekannt zu geben und regelmäßig hierüber zu unterweisen.

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

19 Schlussbemerkung / Dokumentation

Diese Richtlinie wird in regelmäßigen Abständen (mindestens alle 2 Jahre) geprüft und aktualisiert. Bei Änderungswünschen senden Sie bitte eine E-Mail an informationssicherheit@bistum-augsburg.de.

20 Inkrafttreten

Diese Richtlinie tritt zum 01.12.2020 in Kraft.

21 Anlage zur Richtlinie

Verpflichtungserklärung für haupt- und nebenamtliche Mitarbeiter
und Mitarbeiterinnen

Ich (Vor- und Zuname) _____

geboren am _____

wohnhaft in _____

verpflichte mich, die **Benutzerrichtlinie zur Informationssicherheit** in der jeweils geltenden Fassung einzuhalten.

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 Ausdrucks dieser Richtlinie bzw. die Zugangsmöglichkeit (Intranet Portal, Amtsblatt etc.) zu haben.

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

_____ _____

Ort, Datum Unterschrift