Reglement über die Nutzung der Informations- und Kommunikationstechnik (ICT-Nutzungsreglement)

(vom 20. Mai 2019)[1]

Der Synodalrat,

gestützt auf Art. 41 lit. g und k der Kirchenordnung der Römisch-katholischen Körperschaft des Kantons Zürich vom 29. Januar 2009[3], § 7 des Gesetzes über die Information und den Datenschutz vom 12. Februar 2007[2] sowie §§ 39 und 60 der Anstellungsordnung der Römisch-katholischen Körperschaft des Kantons Zürich vom 22. März 2007[4],

beschliesst:

I. Gegenstand

§ 1. [1] Dieses Reglement regelt für alle Mitarbeitenden der Römisch-katholischen Körperschaft des Kantons Zürich die Nutzung der elektronischen Infrastrukturen und die Nutzung von Internet mit Informatikmitteln der Organisation sowie die Nutzung von E-Mail und Sozialen Medien. Zweck

[2] Das Interesse der Körperschaft liegt dabei in der Sicherstellung der Datensicherheit und im Datenschutz, in einer möglichst wenig belasteten betrieblichen Informatikinfrastruktur (Speicherplatz, Netzwerkbandbreite) sowie in finanziellen (der Arbeitnehmer schuldet dem Arbeitgeber seine Arbeitszeit) und ideellen Interessen (Schutz vor Reputationsschäden). Dem stehen das Informations- und Kommunikationsinteresse sowie der Persönlichkeitsschutz der Arbeitnehmenden gegenüber.

[3] Für Dritte, welche die Informatikmittel der Körperschaft nutzen, wird dieses Reglement auf vertraglicher Basis für verbindlich erklärt.

II. Nutzungsvorschriften

Arbeitsinstrumente und Arbeitsergebnis

§ 2. [1] Die geschäftlich anfallenden Daten (Dokumente, E-Mails) sind mit der von der Körperschaft zur Verfügung gestellten Hard- und Software zu bearbeiten und in der betrieblichen Informatikstruktur (Server, Cloud) aufzubewahren.

[2] Nicht ausdrücklich zugelassene Plattformen und Collaboration Tools sind verboten.

[3] Nicht erlaubt sind unverschlüsselte USB-Sticks oder unverschlüsselte externe Festplatten.

[4] Die Installation von Hard- und Software sowie Kommunikationseinrichtungen durch Mitarbeitende ausser den ICT-Verantwortlichen ist untersagt.

[5] Informatiksysteme, die am Netzwerk angeschlossen sind, dürfen nicht gleichzeitig mit einem Netz oder System ausserhalb des internen Netzwerks verbunden werden.

Sicherheitsmassnahmen

§ 3. [1] Das Passwort ist persönlich und darf nicht weitergegeben werden. Passwörter müssen aus mindestens acht Stellen bestehen und sollen eine Kombination von Klein- und Grossbuchstaben, Ziffern und Sonderzeichen enthalten. Leicht zu erratende Passwörter und solche, die einen Bezug zur eigenen Person aufweisen (z. B. Name, Name von Angehörigen, Geburtsdatum usw.), sind nicht erlaubt. Geschäftlich genutzte Passwörter dürfen nicht privat verwendet werden. Passwörter sollten regelmässig gewechselt werden. Sie sind sofort zu ändern, wenn ein Verdacht besteht, dass sie Dritten zur Kenntnis gelangt sind. Ein früher bereits benutztes Passwort darf nicht erneut verwendet werden.

[2] Die Mitarbeitenden dürfen nur ihre persönlichen Benutzerkennungen oder die ihnen zugeteilten funktionellen Kennungen verwenden. Sie sind für die mit ihren Kennungen erfolgten Zugriffe verantwortlich. Der Zugriff auf Daten, die nicht zur Aufgabenerfüllung benötigt werden, ist verboten.

[3] Beim Verlassen des Arbeitsplatzes für längere Zeit ist die Arbeitsstation zu sperren, oder die Benutzerin bzw. der Benutzer meldet sich vom System ab. Laptops und Smartphones sind entsprechend zu sichern, schutzbedürftige Unterlagen vor Zugang zu schützen.

[4] Es ist dafür zu sorgen, dass keine Unbefugten Zutritt zu den Arbeitsräumlichkeiten haben. Halten sich externe Personen in den Büroräumlichkeiten auf, sind Massnahmen zu treffen, die Unbefugten einen Zugang zu Informationen verhindern.

[5] USB-Sticks und externe Festplatten von Dritten sind vor dem Öffnen durch einen Virenschutz zu überprüfen. Es dürfen nur Geräte aus bekannten Quellen verwendet werden.

[6] Die Mitarbeitenden dürfen die Sicherheitssoftware (Virenschutz, Firewall usw.) nicht ausschalten, blockieren oder ihre Konfiguration verändern. E-Mails mit unbekanntem Absender, verdächtigem Betreff oder unüblichem Inhalt sind vorsichtig zu behandeln, da sie von der Virenschutzsoftware nicht erkannte Viren enthalten könnten. Ihre Anhänge sowie Links auf Websites sollen keinesfalls geöffnet werden. Jeder Verdacht auf Virenbefall muss sofort den ICT-Verantwortlichen gemeldet werden.

Daten- und Anwendungssicherheit

§ 4. Zur Wahrung der Daten- und Anwendungssicherheit (Verfügbarkeit, Integrität, Vertraulichkeit) dürfen nur von den ICT-Verantwortlichen der Körperschaft zugelassene Programme installiert werden.

Personendaten und vertrauliche Sachdaten

§ 5. [1] Personendaten und vertrauliche Sachdaten dürfen ausserhalb des körperschaftseigenen Netzwerks oder der iKath-Cloud nur verschlüsselt aufbewahrt werden. Sie dürfen online nicht genannt werden, also nicht im Internet, auch nicht in Sozialen Medien, unverschlüsselten E-Mails oder sonstigen unverschlüsselten Kommunikationsmitteln.

[2] Sie dürfen unverschlüsselt nur im körperschaftseigenen Netzwerk oder innerhalb der iKath-Cloud übertragen werden.

Verwendung von privaten Geräten

§ 6. [1] Geschäftliche Daten dürfen nicht auf privaten PCs, Laptops und Tablets gespeichert oder aufbewahrt werden.

[2] Ausnahmen bewilligt die Generalsekretärin bzw. der Generalsekretär nach Rücksprache mit der Leitung ICT.

[3] Die Bewilligung für private Geräte wird nur erteilt, wenn es unzumutbar ist, ein geschäftliches Gerät zu benutzen und wenn die Sicherheitsmassnahmen gemäss Arbeitsplatzvorgaben erfüllt sind.

[4] Werden Smartphones zu geschäftlichen Zwecken genutzt, müssen sie mit sechsstelligem Passwort, Fingerprint oder Gesichtserkennung gesichert werden. Dokumente mit vertraulichem bzw. schützenswertem Inhalt dürfen nicht gespeichert werden. Enthalten die Geräte schützenswerte Daten, dürfen sie nicht unbeaufsichtigt gelassen oder Dritten zur Nutzung überlassen werden.

Private Nutzung

§ 7. [1] Die private Nutzung von Internet, E-Mail und Sozialen Medien ist während der Arbeitszeit auf ein Minimum zu beschränken und sollte grundsätzlich nur während Pausen erfolgen.

[2] Nicht erlaubt ist das Herunterladen und/oder Speichern von privaten Dateien in grosser Menge / mit grosser Netzwerkbelastung auf den Server (Foto-, Video- und Musikdateien).

[3] Der Zugang zum Internet mit privaten Geräten ist nur im Gästebereich des WLAN erlaubt.

Rechtswidriges

§ 8. Dokumente, Videos und Bilder sowie E-Mails, Webseiten und andere Webinhalte mit rassistischen, pornografischen, sexistischen, gewaltverherrlichenden oder ganz allgemein rechtswidrigen Inhalten dürfen weder konsumiert noch heruntergeladen oder weiterverbreitet werden. Ganz allgemein sind Handlungen, die nach Schweizerischem Strafgesetzbuch unter Strafe stehen, zu unterlassen.

Private E-Mails und Weiterleitung von E-Mails

§ 9. [1] Das Versenden und Empfangen privater E-Mails über das Mail-Konto der Organisation ist erlaubt. Entsprechende E-Mails müssen in einem als «privat» bezeichneten Ordner abgelegt werden. Bei der automatischen Sicherung (Backup) der E-Mails der Arbeitnehmenden werden auch die privaten E-Mails gesichert.

[2] Private E-Mails, die nicht als solche gekennzeichnet sind, gelten als geschäftliche E-Mails.

[3] Nicht erlaubt ist das Publizieren der dienstlichen E-Mail-Adresse auf Webseiten zu privaten Zwecken.

[4] Das automatische Weiterleiten (Forwarding) von E-Mails an die private sowie weitere externe E-Mail-Adressen braucht die Bewilligung der Generalsekretärin bzw. des Generalsekretärs.

[5] Die vorgesetzte Stelle ist bei längerer Abwesenheit (Unfall, Krankheit oder sonstigen ausserordentlichen Ereignissen) einer bzw. eines Mitarbeitenden nach Rücksprache oder versuchter Rücksprache mit der bzw. dem Mitarbeitenden berechtigt, auf deren bzw. dessen E-Mail-Konto zuzugreifen. Sie macht es unter Mitwirkung der Bereichsleiterin bzw. des Bereichsleiters Personal und der bzw. des Datenschutzverantwortlichen.

Respekt

§ 10. Alle Mitarbeitenden der Körperschaft zeigen sich jederzeit respektvoll gegenüber ihren Kommunikationspartnern. Das gilt auch für jene, über die sie allenfalls online schreiben wie Freunde, Arbeitskollegen, Kunden, Kritiker usw., aber auch die katholische Kirche als solche.

Soziale Medien

§ 11. Die Online-Präsenz der Mitarbeitenden beeinflusst auch das Image der Katholischen Kirche im Kanton Zürich. In persönlichen Blogs oder Einträgen und Profilen in Sozialen Netzwerken wie z. B. Facebook soll aus den Umständen klar ersichtlich werden, dass hier die Privatperson ihre eigene Meinung vertritt. Sofern das nicht sowieso aus den Umständen deutlich erkennbar ist, müssen die Mitarbeitenden einen Hinweis darauf anbringen, dass die geäusserten Meinungen alleine jene der Autorin bzw. des Autors sind und nicht die Sicht der Katholischen Kirche im Kanton Zürich repräsentieren.

III. Organisation

ICT-Verantwortung

§ 12. [1] Die ICT-Verantwortung obliegt dem Synodalrat.

[2] Die operative Verantwortung obliegt der Generalsekretärin bzw. dem Generalsekretär, technisch zuständig ist die ICT-Stabsstelle.

[3] Verwaltung, Generalvikariat, Fach- und Dienststellen und Missionen haben je eine Ansprechperson für Informations- und Kommunikationstechnik (ICT). Wird keine bezeichnet, ist diese die Stellenleiterin bzw. der Stellenleiter.

[4] Die ICT-Stabsstelle der Verwaltung unterstützt die Ansprechpersonen und hat einen Überblick über die Verwendung der Hard- und Software in der Körperschaft. Die Einzelheiten regelt der Synodalrat in einem ICT-Konzept.

Betreiberstelle

§ 13. [1] Als Betreiberstellen gelten die Informatikdienste, die für den Betrieb der elektronischen Infrastruktur und der Dienste der Körperschaft zuständig sind.

[2] Durch Vertrag oder Weisung wird sichergestellt, dass die Betreiberstellen die rechtskonforme und sichere Nutzung der elektronischen Infrastruktur und der Dienste der Körperschaft ermöglichen.

Zuständigkeit ICT-Stabsstelle Verwaltung

§ 14. [1] Die ICT-Stabsstelle der Verwaltung ist zuständig für den Betrieb des körperschaftseigenen Servers in der Verwaltung und die an ihn angeschlossenen Peripheriegeräte.

[2] Sie ist mithilfe der Betreiberstelle insbesondere zuständig für:

a. die Installation eines Spam-Filters und die Löschung als Spam erkannter Daten,
b. das Speichern sämtlicher E-Mails im E-Mail-Journal,
c. die Bewilligung von Software gemäss §§ 2 und 4,
d. das Sperren und Freischalten von Internetseiten im Einvernehmen mit der Generalsekretärin bzw. dem Generalsekretär,
e. bei Bedarf anonyme Auswertungen gemäss § 16,
f. bei Bedarf personenbezogene Auswertungen gemäss § 21.

[3] Bei ausserordentlichen Ereignissen (wie technische Störung oder Netzwerküberlastung) kann die ICT-Stabsstelle den Datenverkehr vorübergehend einschränken. Eine solche Massnahme wird im Intranet mitgeteilt.

Zugang zu geschäftlichen Daten bei Abwesenheiten

§ 15. [1] Die vorgesetzte Stelle ist bei längerer Abwesenheit einer bzw. eines Mitarbeitenden (Unfall, Krankheit oder sonstigen ausserordentlichen Ereignissen) berechtigt, nach Rücksprache oder versuchter Rücksprache auf deren bzw. dessen geschäftliche Daten zuzugreifen. Sie macht es unter Mitwirkung der Bereichsleiterin bzw. des Bereichsleiters Personal und der bzw. des Datenschutzverantwortlichen.

[2] Geschäftliche Daten werden der vorgesetzten Stelle ausgehändigt, private Dateien bleiben in der Datenablage der betroffenen Person. Die Vertraulichkeit und der Schutz privater Dateien kann nicht gewährleistet werden.

Anonymisierte Berichte

§ 16. [1] Die Betreiberstellen erstellen auf Verlangen der Generalsekretärin bzw. des Generalsekretärs anonymisierte Berichte, die Aufschluss über die angewählten Internetadressen und soweit möglich über Zeitpunkt und Anzahl der Zugriffe und übertragenen Datenmengen geben.

[2] Die Berichte dürfen keine Rückschlüsse auf einzelne Mitarbeitende zulassen. Insbesondere dürfen sich aus ihnen weder die einzelnen Mitarbeitenden noch die einzelnen Arbeitsplätze ergeben.

IV. Missbrauch der elektronischen Infrastrukturen und Dienste der Körperschaft

Überwachungsmassnahmen

§ 17. Gegen Missbrauch und technische Schäden setzt die Körperschaft technische Schutzmassnahmen (z. B. Sperren bestimmter Webdienste, Installieren von Anti-Virensoftware usw.) ein. Auch die anonymisierte technische Überwachung des Internetverkehrs ist gemäss § 16 zulässig. Besteht der begründete Verdacht, dass trotz technischen Schutzmassnahmen gegen dieses Reglement verstossen wird, erfolgt eine personenbezogene Überwachung und Auswertung der Internet- und E-Mail-Protokollierungen. Der Einsatz von Spionageprogrammen ist dabei verboten.

Definition

§ 18. Ein Missbrauch im Sinne dieses Reglements besteht bei einem Verstoss gegen §§ 2–8.

Entscheid über personenbezogene Berichte

§ 19. [1] Zuständig für die Anordnung einer personenbezogenen Auswertung ist die Generalsekretärin bzw. der Generalsekretär. Sie bzw. er trifft den Entscheid zusammen mit der Bereichsleiterin bzw. dem Bereichsleiter Personal und der bzw. dem Datenschutzverantwortlichen der Körperschaft.

[2] Die Voraussetzungen für die Anordnung einer personenbezogenen Auswertung sind erfüllt, wenn

– bei Internetzugriffen Missbräuche von erheblicher Tragweite vorliegen oder
– beim E-Mail-Verkehr ein konkreter Verdacht auf Missbrauch besteht.

Ankündigung der personenbezogenen Berichte

§ 20. Die Generalsekretärin bzw. der Generalsekretär weist die betroffenen Mitarbeitenden darauf hin, dass für einen bestimmten Zeitraum die Internetzugriffe oder der E-Mail-Verkehr personenbezogen protokolliert und ausgewertet werden.

Durchführung

§ 21. [1] Nach erfolgter Ankündigung kann die Generalsekretärin bzw. der Generalsekretär die Betreiberstellen beauftragen, personenbezogene Berichte über die Internetzugriffe oder den E-Mail-Verkehr zu erstellen.

[2] Personenbezogene Berichte dürfen für höchstens drei Monate erstellt werden. Über den Zeitraum vor der Ankündigung durch die Generalsekretärin bzw. den Generalsekretär dürfen keine personenbezogenen Berichte erstellt oder ausgewertet werden.

[3] Die Betreiberstelle stellt die als vertraulich deklarierten Berichte der Generalsekretärin bzw. dem Generalsekretär zu.

Inhalt

§ 22. [1] Personenbezogene Berichte über den Internetzugriff enthalten

– den Namen der Internetnutzerin oder des Internetnutzers,
– die angewählten Internetadressen,
– soweit möglich den Zeitpunkt und die Anzahl der Zugriffe sowie die übertragene Datenmenge.

[2] Personenbezogene Berichte über den E-Mail-Verkehr enthalten

– den Namen der E-Mail-Nutzerin oder des E-Mail-Nutzers,
– die angewählten Adressen,
– den Versandzeitpunkt,
– die Datenmenge der ausgehenden E-Mails.

Einleitung von Massnahmen

§ 23. [1] Die Generalsekretärin bzw. der Generalsekretär entscheidet zusammen mit der Bereichsleiterin bzw. dem Bereichsleiter Personal und der bzw. dem Datenschutzverantwortlichen der Körperschaft aufgrund der personenbezogenen Berichte, ob dem Personalausschuss beantragt wird, gegen die betreffende Person eine Administrativuntersuchung durchzuführen, oder ob andere Massnahmen zu treffen sind.

[2] Die Generalsekretärin bzw. der Generalsekretär teilt der betreffenden Person den Entscheid mit.

Prüfung und Vernichtung der Unterlagen

§ 24. Wird keine Administrativuntersuchung eingeleitet, werden die personenbezogenen Berichte und Protokolle nach 30 Tagen vernichtet und die Mitarbeitenden informiert.

V. Schlussbestimmungen

Kenntnisnahme des Reglements

§ 25. Jede Mitarbeiterin und jeder Mitarbeiter unterzeichnet das Reglement als Erklärung, dass sie bzw. er das Reglement gelesen und verstanden hat und die Nutzungsvorschriften einhalten wird.

Inkrafttreten

§ 26. Dieses Reglement tritt am 1. Oktober 2019 in Kraft.

[1] OS 74, 488; Begründung siehe ABl 2019-06-14.
[2] LS 170.4.
[3] LS 182.10.
[4] LS 182.41.