Graz, 10. April 2018
Ord.-Zl.: 1 Di 4-18

Informationssicherheitsrichtlinie der Diözese Graz-Seckau und ihrer Einrichtungen

Dieses Dokument adressiert den Schutz von Information, Daten und IT, insbesondere im Kontext des Datenschutzes.

Inhalt

1 Zweck und Inhalt

Diese Richtlinie der Diözese Graz-Seckau (DGS) adressiert den Schutz von Information, Daten und IT, insbesondere im Kontext des Datenschutzes.

Sie dient dem Schutz personenbezogener, genauso wie sonstiger schutzwürdiger Daten und Informationen in analoger und elektronischer Form und umfasst organisatorische und technische Maßnahmen.

Diese Richtlinie wurde vom Diözesanbischof mit 1. Mai 2018 in Kraft gesetzt und den im Geltungsbereich Genannten bekanntgemacht.

2 Geltungsbereich

Diese Richtlinie gilt für Mitglieder des Klerus und für haupt- und ehrenamtlich Tätige der Diözese Graz-Seckau - im Folgenden DGS genannt - und aller Einrichtungen, die dem Diözesanbischof unterstehen.

Dritte sind in den jeweils relevanten Punkten zu verpflichten.[1]

Darüber hinaus gilt diese Richtlinie ohne zeitliche und örtliche Einschränkungen.

3 Ziele

Angestrebt werden von der DGS die folgenden, gleichwertigen Sicherheitsziele:

- Schutz vor Verlust und Zerstörung von Information (Verfügbarkeit)
- Schutz vor unberechtigtem Zugriff, unbefugter Kenntnisnahme und Preisgabe von Information (Vertraulichkeit)
- Schutz vor ungewollter und manipulativer Veränderung von Information (Integrität)
- Schutz vor Verlust der Nachvollziehbarkeit bzw. Gewährleistung der Nichtabstreitbarkeit von Informationsflüssen
- Sicherstellung der Kontinuität des Betriebs.
- Schutz aller personenbezogenen und geschäftsbezogenen Daten und Informationen
- Schadensvermeidung und Schadensbegrenzung durch vorbeugende Sicherheitsmaßnahmen
- Förderung eines umfassenden Sicherheitsbewusstseins und einer Sicherheitskultur
- Einhaltung gesetzlicher Vorgaben und vertraglicher Vereinbarungen

4 Rollen, relevante Dokumente und Begriffsbestimmungen

Rollen:

- Kirchliche Datenschutzkommission (der Österreichischen Bischofskonferenz)

[1] Z.B. sind Zivildiener, Praktikanten und Poolkräfte mittels Vertraulichkeitsvereinbarungen, Verpflichtungserklärungen oder Ähnlichem auf diese Richtlinie zu verpflichten.

- Datenschutzbeauftragte/r der Katholischen Kirche in Österreich gemäß DSGVO
- Bereichsdatenschutzreferent/in der Diözese Graz-Seckau (für die DGS zuständig)
- Datenschutzzuständige/r der Einrichtungen (für Einrichtungen der DGS zuständig)

Relevante Dokumente:

- Decretum Generale über den Datenschutz in der Katholischen Kirche in Österreich und ihren Einrichtungen (kirchliche Datenschutzverordnung)
- Datenschutzrichtlinie der Katholischen Kirche Österreich
- Informationssicherheitsrichtlinie der DGS

Definitionen:

Im Kontext dieses Dokuments werden Begriffe wie folgt definiert:

IT-Endbenutzer

Personen, die aus dem in dieser Richtlinie definierten Geltungsbereich stammen und eines der unten definierten IT-Arbeitsmittel und damit in Verbindung stehende (mobile) Datenträger nutzen.

IT-Arbeitsmittel

Unter IT-Arbeitsmitteln werden verstanden: Hardware, d.h. IT-Endgeräte, IT-Peripheriegeräte, IT-Zubehör, Datenträger etc. sowie Software auf den IT-Geräten, außerdem Geräte wie Telefonapparate, Funkgeräte etc.

IT-Endgeräte

Standgeräte (Desktops), tragbare Geräte (Notebooks, Tablet PCs, Tablets etc.), netzwerkfähige Kleingeräte (Smartphones, Navigationsgeräte, Datenerfassungsgeräte, VoIP Telefone etc.), Mobiltelefone, Multifunktionsgeräte (Kombifaxe, Druck(Fax)stationen etc.).

Mobile Datenträger

Speichersticks (USB-Sticks), Speicherkarten aller Art (auch in Multimedia-Abspielgeräten, in Kameras etc.), mobile Festplatten (z.B. magnetisch und flashspeicher-basiert), CDs, DVDs, Disketten, Magnetbänder und ähnliche Speichermedien.

Freigegebene Hardware und Software

Darunter werden IT-Endgeräte, mobile Datenträger, Betriebssysteme, Anwendungen etc. verstanden, die bestimmten, von DGS festgelegten Kriterien entsprechen.

Erlaubnistatbestände im Sinne der DSGVO:

1. Einwilligung (Art 6, Abs 1, lit a DSGVO)
2. Zur Vertragserfüllung erforderlich (Art 6, Abs 1, lit b DSGVO)

3. Zur Erfüllung einer rechtlichen Verpflichtung, welcher der Verantwortliche unterliegt, erforderlich (Art 6, Abs 1, lit c DSGVO)
4. Erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen (Art 6, Abs 1, lit d DSGVO)
5. Verarbeitung liegt im öffentlichen Interesse oder erfolgt in Ausübung öffentlicher Gewalt (Art 6, Abs 1, lit e DSGVO)
6. Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich und Interessen oder Grundrechte und Grundfreiheiten des Betroffenen überwiegen nicht (Art 6, Abs 1, lit f DSGVO)

5 Regelungen

5.1 Zulässige Verarbeitung von personenbezogenen Daten

Personenbezogene Daten

- dürfen nur im absolut notwendigen Ausmaß und für festgelegte, eindeutige und rechtmäßige Zwecke verarbeitet werden[2];
- dürfen nur dann verarbeitet werden, wenn zumindest ein entsprechender Erlaubnistatbestand vorliegt;
- dürfen nur solange und im vollen Umfang gespeichert werden, wie es für die Zweckerfüllung notwendig ist;
- müssen sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein.

Im Zweifel ist Rücksprache mit der zuständigen datenschutzverantwortlichen Person (Referent/in, Datenschutzzuständige/r) zu halten.

Bei der Planung eines Projekts, in dem personenbezogene Daten verarbeitet werden sollen, ist mit der zuständigen datenschutzverantwortlichen Person (Referent/in, Datenschutzzuständige/r) Rücksprache zu halten und bei allfälliger Aufnahme einer Verarbeitung personenbezogener Daten die Zustimmung durch den/die Bereichsdatenschutzreferenten/in einzuholen.

Die Weitergabe von personenbezogenen Daten an Lieferanten und sonstige Dritte zu Test- und Wartungszwecken, z.B. im Zusammenhang mit Software-Entwicklung oder Fehlerbehebung, ist untersagt.

Von allen im Geltungsbereich dieses Dokuments umfassten Personen ist eine Verpflichtungserklärung gemäß § 6 DSG 2018 (Datengeheimnis) zu unterfertigen und per E-Mail an datenschutz@graz-seckau.at zu übermitteln.

[2] Erklärung: Beispielsweise ist das Sammeln von personenbezogenen Daten auf Vorrat zum Zwecke späterer Auswertung nicht zulässig, ebenso das spätere Verwenden für andere Zwecke, wobei Zwecke generell eng zu interpretieren sind.

5.2 Schutz der Arbeitsumgebung

5.2.1 Der Arbeitsplatz ist von den Mitarbeiter/inne/n so zu gestalten, dass hierfür nicht berechtigte Besucher oder sonstige Dritte keinen Zugang zu personenbezogenen Daten bekommen können.

5.2.2 Bei jedem Verlassen des Notebooks, Desktop- und Tablet-PCs oder Terminals ist der Sperrbildschirm manuell zu aktivieren.

5.2.3 Bildschirme sind so auszurichten und Informationen in Papierform so abzulegen, dass das Risiko der Einsicht durch Unbefugte nach Möglichkeit ausgeschlossen wird.

5.2.4 Die Nutzung eines dienstlichen IT-Endgeräts durch andere Personen als die berechtige(n) Person(en) ist nicht gestattet.

5.2.5 Die dienstliche Nutzung von privaten IT-Endgeräten ist untersagt.

5.2.6 Die Veränderung von sicherheitsrelevanten Einstellungen ist untersagt.[3]

5.2.7 Erlaubt ist nur der Einsatz von Software, die von der IT-Abteilung freigegeben ist, d.h. die eigenständige Installation von Software ist untersagt.

5.2.8 Die Speicherung von Daten ist ausschließlich auf zentralen Speicherbereichen (Netzwerklaufwerken) zulässig, wo sie automatisch regelmäßig gesichert werden.

5.2.9 Alltägliche Arbeiten an PCs und Notebooks sind mit Standardbenutzerrechten auszuüben.

5.3 Synchronisation mobiler IT-Endgeräte

Sofern eine Synchronisation von E-Mails, Kontakten, Kalendern und Aufgaben mit dem DGS Server erfolgen soll, gelten folgende Regeln:

- Das mobile IT-Endgerät muss über das MDM (Mobile Device Management-System) registriert und verwaltet werden.
- Die Synchronisation ist ausschließlich mit der von der IT vorgegebenen App möglich.
- Individuelle Installationen von Apps sind möglich, da sich alle Unternehmensdaten von Mail, Kalender, Aufgaben und Kontakten in einem sicheren Container befinden (MAM-Mobile Application Management) und somit nicht mit anderen Apps interagieren können.
- Minimalanforderungen an Software-Versionen der Mobilgeräte und ein gewisser Patch-Level sind notwendig, damit die Installation der MDM- und MAM-Apps möglich ist. Geräte, die über einen Jailbreak verfügen oder auf Root gesetzt worden sind, werden nicht zugelassen.

[3] Z.B. das Einschränken oder Verhindern der automatischen Installation von Sicherheitsupdates oder das Entfernen eines Passworts.

- Der Container ist nach dem aktuellen Stand der Technik verschlüsselt und durch einen PIN-Code gesichert, der vom Benutzer/der Benutzerin frei gewählt werden kann.
- Der Container wird nach einer vorgegebenen Zeit der Inaktivität automatisch gesperrt.
- Innerhalb des Containers ist ein Schutz vor Schadsoftware gegeben.
- Der Container samt Unternehmensinhalt kann, wenn nötig, vom Administrator mittels Fernzugriff deaktiviert oder gelöscht werden.

5.4 Unterwegs mit IT

Mobile IT-Endgeräte müssen unter ständiger Kontrolle der berechtigten Person(en) bleiben, d.h. sie dürfen nicht unbeaufsichtigt gelassen werden. Ist es unvermeidbar, IT-Endgeräte in einem Auto aufzubewahren, so müssen diese von außen nicht sichtbar im Kofferraum aufbewahrt werden.

Der Verlust oder Diebstahl eines mobilen IT-Endgeräts ist unverzüglich der DGS Ausgabestelle zu melden.

5.5 Datenaustausch über Datenträger

Die Verwendung von unverschlüsselten SD-Karten ist untersagt, außer diese befinden sich entweder unter ständiger Aufsicht durch den berechtigten Benutzer/die berechtigte Benutzerin und werden bei Nichtgebrauch an einem entsprechend sicheren Ort vor unberechtigtem Zugriff geschützt aufbewahrt.

Die Verwendung von USB-Sticks und externen Festplatten ist nur unter nachfolgenden Bedingungen erlaubt:

- Es werden ausschließlich verschlüsselte Datenträger verwendet.
- Die USB-Sticks werden von der IT-Abteilung ausgegeben, externe Festplatten werden von der IT-Abteilung verschlüsselt.
- Jeder Datenträger wird mit einem Verschlüsselungspasswort versehen, das von der berechtigten Person gewählt wird.
- Es wird ein Bestandsverzeichnis über die eingesetzten Datenträger geführt, um eine eindeutige Zuordnung zu ihren Nutzern zu ermöglichen.
- Die Nutzung erfolgt ausschließlich zu dienstlichen Zwecken.
- Die Datenträger werden an einem entsprechend sicheren Ort vor unberechtigtem Zugriff geschützt aufbewahrt.

Der Verlust oder Diebstahl eines Datenträgers, der dienstliche Daten enthält, ist unverzüglich der jeweiligen DGS-Ausgabestelle zu melden.

5.6 Nutzung von Cloud-Diensten

Es ist ausschließlich der hausinterne Cloud-Dienst zu verwenden, der alle Daten nur auf diözesanen Servern speichert. Die Speicherung in anderen Cloud-Diensten ist verboten.[4] Alle Regelungen zum Schutz personenbezogener Daten gelten auch in diesem Umfeld.

5.7 E-Mail und Internet

Besondere Kategorien personenbezogener Daten[5] („sensible Daten“) dürfen ausschließlich über verschlüsselte Verbindungen übermittelt werden. Dazu ist bevorzugt der hausinterne Cloud-Dienst zu verwenden, wobei per E-Mail ausschließlich der Link zu den dort abgelegten Daten versendet werden darf.

Die private Nutzung der dienstlichen E-Mail-Adresse ist untersagt.

Die private Internet-Nutzung ist eingeschränkt gestattet (für Beschäftigte im Bischöflichen Ordinariat ist anzuwenden: BV Internet, E-Mail und IT-Betriebsmittel. Für alle anderen Personen ist die BV sinngemäß ebenfalls verpflichtend anzuwenden.).

Die Speicherung privater Daten ist untersagt.

5.8 Passwortschutz

Die Passwörter sind so zu wählen, dass sie nicht leicht zu erraten sind.

Passwörter sind vom berechtigten Benutzer/der berechtigten Benutzerin geheim zu halten und dürfen nicht weitergegeben werden, auch nicht z.B. an Dienstvorgesetzte, Vertretungen oder Assistent/inn/en. Auf eine unbeobachtete Eingabe des Passworts ist zu achten.

Passwörter, von denen angenommen werden muss, dass sie Unberechtigten bekannt geworden sein könnten oder sind, müssen vom berechtigten Benutzer/der berechtigten Benutzerin geändert werden bzw. muss von diesem/dieser eine Passwortrücksetzung veranlasst werden.

Meldet sich ein Benutzer/eine Benutzerin über ein externes, nicht von der DGS betriebenes System an einem System der DGS an, so muss er/sie sich unmittelbar nach Benützung wieder abmelden und dafür Sorge tragen, dass die Benutzerdaten aus dem System gelöscht sind

Ist es erforderlich, Passwörter zu notieren, so sind diese vom/der Benutzer/in so zu verwahren, dass sie ausschließlich diesem/dieser zugänglich sind.

---

[4] Wie z.B. Dropbox oder iCloud.

[5] Diese sind personenbezogene Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

5.9 Entsorgung von Speichermedien

Vertrauliche und interne Unterlagen in Papierform sind mittels Aktenvernichter oder durch kleinteiliges Zerschneiden zu zerstören oder in den dafür vorgesehenen Datenschutzcontainer zu entsorgen.

Vor Beendigung des Arbeitsverhältnisses oder Außerbetriebnahme eines IT-Endgeräts oder mobilen Datenträgers sind von der DGS bereitgestellte IT-Arbeitsmittel je nach Art an die dafür vorgesehene Stelle zu retournieren, die auch die Vernichtung und sichere Entsorgung oder die Neukonfiguration zur Weiterverwendung übernimmt.

5.10 Fotos und Video

Zur Verwendung und Veröffentlichung von Bilddaten ist die Zustimmung des/der Betroffenen einzuholen und sind insbesondere die Regelungen im Kapitel „Zulässige Verarbeitung von personenbezogenen Daten“ zu beachten.

5.11 Social Media

Die Nutzung von Social Media zu dienstlichen Zwecken ist nur auf Basis der vorliegenden Richtlinie erlaubt:

- Nutzer/innen halten sich an geltendes Recht und berücksichtigen bei allen Veröffentlichungen insbesondere Persönlichkeitsrechte.
- Vertrauliche und interne Informationen werden nicht kommuniziert.
- Nutzer/innen treten ausschließlich mit eigenem Namen auf, geben DGS und Funktion an und sorgen für eine Kontaktmöglichkeit.
- Nutzer/innen akzeptieren die Meinungsfreiheit in Social Media, veröffentlichen keine beleidigenden oder diskriminierenden Inhalte und üben öffentlich keine Kritik an DGS und deren Partnern, Kunden und Lieferanten.

5.12 Urheber- und Markenrechte[6]

Urheber- und Markenrechte sind zu wahren und Lizenzbestimmungen sind einzuhalten.

5.13 Umgang mit Bewerbungen

Bewerbungsunterlagen dürfen in der DGS nur den Personen zugänglich gemacht werden, die mit der Besetzung der Vakanz direkt befasst sind. Alle Bewerbungsunterlagen werden ausschließlich in Papierform zur Einsicht gegen Abgabe einer schriftlichen Erklärung zur Einhaltung des Datenschutzes und Verbot jeglicher Abschriften (Kopie, Fotografie etc.) im Original der/dem Verantwortlichen für die Stellenbesetzung übergeben. Alle Bewerbungsunterlagen sind wieder vollständig an die organisatorisch zuständige Stelle (z.B. in der DGS dem Personalbüro) zurückzugeben. Dies gilt analog für kirchliche Einrichtungen.

Personenbezogene Daten müssen dauerhaft gelöscht werden, sobald eine Vakanz neu besetzt und die Speicherung der Bewerberdaten somit nicht mehr notwendig ist.

[6] http://medien.katholisch.at/urheberrecht

Unterlagen sind spätestens sechs Monate nach Ablehnung zu vernichten, sofern es mit dem Bewerber keine gesonderte schriftliche Vereinbarung zur Evidenzhaltung gibt.

6 Pflichten des Einzelnen

Voraussetzung zur Erreichung der Informationssicherheitsziele ist ein gewissenhafter und sorgfältiger Umgang mit Daten, Informationen und informationsverarbeitenden Systemen durch alle Beschäftigten der DGS und hinzugezogene Dritte. Eine besondere Bedeutung kommt dabei der Vorbildfunktion von Führungskräften aller Ebenen zu.

Darüber hinaus sind Führungskräfte verpflichtet, die Maßnahmen zur Sicherstellung der Informationssicherheit in ihrem unmittelbaren Wirkungskreis nachhaltig umzusetzen.

7 Folgen der Nichteinhaltung

Eine Missachtung von Sicherheitsbestimmungen kann neben entsprechenden disziplinären und dienstrechtlichen auch zivil- und strafrechtliche Folgen nach sich ziehen.

8 Meldung von Sicherheitsschwachstellen und -vorfällen

Sicherheitsvorfälle und Sicherheitsschwachstellen sind an den Bereichsdatenschutz-referenten zu melden.

9 Übergangsbestimmungen

Um der Caritas der Diözese Graz-Seckau die notwendigen organisatorischen Maßnahmen zu ermöglichen, treten die Punkte 5.2.5, 5.2.7 sowie 5.7 spätestens mit 1. Jänner 2020 in Kraft.

10 Aufhebung bisheriger Regelungen

Mit Inkrafttreten dieser Informationssicherheitsrichtlinie treten alle bisherigen diesbezüglichen Regelungen - mit Ausnahme der Richtlinie „Videoüberwachung in kirchlichen denkmalgeschützten Gebäuden“ veröffentlicht im KVBl 2011 II 18. - außer Kraft.

Bischof

Kanzler