KATHOLISCHE KIRCHE STEIERMARK

INFORMATIONSSCHUTZ IM KONTEXT DER EU DATENSCHUTZ-GRUNDVERORDNUNG (DSGVO) UND DES DATENSCHUTZGESETZES (DSG 2018)

Informations-, IT- und Datensicherheit bei der Diözese Graz-Seckau

– Zur internen Verwendung bei der Diözese Graz-Seckau –

Stand: 18.04.2018

Inhaltsverzeichnis

Der Pfeil rechts auf jeder Seite bedeutet: Zurück zum Inhaltsverzeichnis. Wenn gelb: außerdem Kapitelende

Wichtige Begriffe in dieser Unterlage

- **Datenschutz**: Stellt sicher, dass die Verarbeitung von Daten rechtmäßig, d.h. gesetzeskonform, erfolgt. Grundlagen sind die DSGVO (EU Datenschutz-Grundverordnung) und das Datenschutzgesetz.
- **Datensicherheit**: Umfasst in Bezug auf personenbezogene Daten jene Sicherheitsmaßnahmen, die den gesetzlichen Datenschutz gewährleisten, insbesondere Zugangsschutz, der auch den Zutrittsschutz umfasst, sowie Zugriffsschutz.
- **IT-Sicherheit**: Bezweckt den Schutz von elektronisch verarbeiteten Daten und der zur Datenverarbeitung verwendeten IT-Systeme.
- **Informationssicherheit**: Bezweckt den Schutz von Daten und Informationen in jeglicher Form, d.h. auf Papier, gesprochen und elektronisch und in sonstiger Weise gespeichert und verarbeitet.
- **IT-Endgerät**: Standgeräte (Desktops, Thin Clients), tragbare Geräte (Notebooks, Tablet PCs, Tablets etc.), netzwerkfähige Kleingeräte (Smartphones, Mobiltelefone, Datenerfassungsgeräte, VoIP Telefone etc.)
- **Mobiler Datenträger**: Speichersticks (USB-Sticks), Speicherkarten aller Art, mobile Festplatten (z.B. magnetisch und flashspeicher-basiert), CDs, DVDs und ähnliche Speichermedien.
- **BYOD** (Bring Your Own Device): Mitarbeiter/innen verwenden private Geräte für dienstliche Zwecke, z.B. um dort E-Mails zu empfangen. Erfordert die Zustimmung des Arbeitgebers.
- **Schadsoftware**: Programme, die vorsätzlich schädigende Funktionen ausführen. Der Begriff bezeichnet also keine schadhafte, sondern gewollt schädigende Software. Das kann z.B. das Löschen von Dateien sein, das Verschlüsseln von Daten und Erzwingen von Lösegeldzahlungen oder das Einnisten von Software zum Zweck des Ausspähens von Tastaturanschlägen, z.B. bei der Passworteingabe.

Welche Daten sind zu schützen — insbesondere bezüglich Vertraulichkeit?

Daten, die insbesondere nach der DSGVO (EU Datenschutz-Grundverordnung) und dem Datenschutzgesetz zu schützen sind:

- Alle Daten zu natürlichen Personen, wenn diese dadurch identifiziert werden oder identifiziert werden können, z.B. Name, Wohnadresse, Geburtsdatum, Sozialversicherungsnummer, Lebenslauf, Einkommen, Abbild, Fingerabdrücke, Gewicht, Stimme etc. — und besondere Kategorien von Daten („sensible Daten“).

Beispiele:

- Daten der Beitragszahlenden
- Daten der Mitarbeiter/innen
- Kundendaten und Lieferantendaten
- Klient/inn/endaten

Nahezu alle verarbeiteten Daten und Informationen der DGS sind auch über die DSGVO und das Datenschutzgesetz hinaus schützenswert — sie alle stellen bedeutende Werte für die DGS dar.

Die DSGVO und das Datenschutzgesetz schützen Daten betreffend natürliche Personen, also Menschen.
Das Datenschutzgesetz 2000 wird am 25.05.2018 durch die DSGVO und das Datenschutzgesetz 2018 abgelöst.

Wichtige Informationen zu den Schutzmaßnahmen abhängig von der Art der Daten finden Sie in der „Informationssicherheitsrichtlinie der Diözese Graz-Seckau und ihrer Einrichtungen“. Dort erfahren Sie, wann Daten z.B. verschlüsselt und wie z.B. USB-Sticks entsorgt werden müssen. Die Schlüsselparagrafen sind Artikel 32 der DSGVO und § 6 des Datenschutzgesetzes. Näheres dazu auf den nächsten Seiten.

Die DSGVO — wichtige Begriffe 1/2

Die DSGVO (EU-Datenschutz-Grundverordnung) definiert:

Personenbezogene Daten: alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.

Besondere Kategorien von Daten (besonders schutzwürdige Daten; früher: sensible Daten): personenbezogene Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

Verarbeitung: jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

Verletzung des Schutzes personenbezogener Daten: eine Verletzung der Sicherheit, die zur Vernichtung, zum Verlust oder zur Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden.

Die DSGVO — wichtige Begriffe 2/2

Die DSGVO (EU-Datenschutz-Grundverordnung) definiert:

Verantwortlicher: die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

Auftragsverarbeiter: eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet (Anm.: also nicht für eigene Zwecke verwenden darf).

Betroffen(e)r: jede natürliche Person, deren Daten verarbeitet werden.

Empfänger: eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, denen personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht. Behörden, die im Rahmen eines bestimmten Untersuchungsauftrags nach dem Unionsrecht oder dem Recht der Mitgliedstaaten möglicherweise personenbezogene Daten erhalten, gelten jedoch nicht als Empfänger; die Verarbeitung dieser Daten durch die genannten Behörden erfolgt im Einklang mit den geltenden Datenschutzvorschriften gemäß den Zwecken der Verarbeitung.

Dritter: eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten.

Datensicherheit gemäß DSGVO Artikel 32 — Verantwortlichkeiten

Die DSGVO verlangt:

- Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.
- Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind – insbesondere durch Vernichtung, Verlust oder Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder durch unbefugte Offenlegung beziehungsweise unbefugtem Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden.

Mitarbeiter/innen tragen eine entsprechende Teilverantwortung.

Anwendungsbeispiele für Sicherheitsmaßnahmen:

Stellenbeschreibungen, Berechtigungsvergabe, Datensicherung, Passwörter, Portier/Empfang und Gebäudesicherung, abschließbare Kästen, Protokollierung, Dokumentation.

Die DSGVO und das Datenschutzgesetz — klipp & klar

Zugangsschutz ist zu gewährleisten, die Zugriffsberechtigung auf Daten und Programme sowie der Schutz der Datenträger vor der Einsicht und Verwendung durch Unbefugte sind zu regeln und jedes Gerät ist durch Vorkehrungen bei den eingesetzten Maschinen oder Programmen gegen die unbefugte Inbetriebnahme abzusichern.

Die Sicherheitsmaßnahmen müssen unter Berücksichtigung des Stands der Technik und der zur Absicherung notwendigen Kosten ein Schutzniveau gewährleisten, das den Risiken, die von der Verarbeitung der Daten ausgehen, und der Art der zu schützenden Daten angemessen ist.

⇨ *Risikoabschätzungen sind für die DGS das Mittel der Wahl zur Feststellung der Angemessenheit.*

Welche Daten- und IT-Sicherheitsmaßnahmen sind gemäß DSGVO/Datenschutzgesetz von der DGS zu setzen?

- Festlegen der Aufgabenverteilung in der DGS betreffend die Datenverwendung
- Binden der Datenverwendung an rechtsgültige Aufträge/Anordnungen weisungsbefugter Stellen in der DGS
- Belehren aller Mitarbeiter/innen über die bestehenden Vorschriften und Pflichten (gesetzlich und DGS-intern)
- Regeln der Zutrittsberechtigung zu den Räumlichkeiten der DGS
- Regeln der Zugriffsberechtigung auf Daten und Programme und Treffen von Vorkehrungen zum Schutz der Datenträger (inkl. Papier) vor unbefugtem Zugriff
- Festlegen der Berechtigung zum Betrieb von Datenverarbeitungsgeräten und Absicherung der Geräte und Programme vor unbefugter Inbetriebnahme
- Führen von Protokollen in Bezug auf z.B. Änderungen, Abfragen und Übermittlungen von personenbezogenen Daten
- Dokumentieren aller obigen Maßnahmen

Diese Anforderungen betreffen insbesondere Führungskräfte.

Welche Datensicherheitsmaßnahmen muss ich setzen?

Einige **Beispiele**:

- Setzen eines Geräte-PIN z.B. am Smartphone oder Tablet
- Verwenden eines „angemessen sicheren“ Passworts unter Windows
- Shredden von Papier
- Speichern von dienstlichen personenbezogenen Daten nur auf Geräten der DGS
- Verwenden von Vertraulichkeitsvereinbarungen mit Externen
- Verwenden von z.B. USB-Sticks und mobilen Datenträgern nur mit Verschlüsselung — USB-Sticks mit integrierter Verschlüsselung können Sie über die IT-Abteilung beziehen
- Manuelles Aktivieren des Sperrbildschirms bei Verlassen des Arbeitsplatzes
- Versperren der Bürotüre
- Verwenden des Zimmersafes in Hotels, z.B. für das Notebook

Details und weitere Maßnahmen finden Sie weiter hinten in diesem Foliensatz.

Außerdem finden Sie wichtige Informationen zum Umgang mit schutzbedürftigen Daten in der „ Informationssicherheitsrichtlinie der Diözese Graz-Seckau und ihrer Einrichtungen“. Dort erfahren Sie, wann Daten z.B. verschlüsselt oder wie z.B. USB-Sticks entsorgt werden müssen.

Weitere Beispiele für Sicherheitsmaßnahmen zur Umsetzung der DSGVO und des Datenschutzgesetzes

Einige weitere **Beispiele**:

- Berechtigungskonzepte
- PINs bei Apps mit besonders sensiblen Daten
- Portier/Empfang
- Abschließbare Kästen
- Vertraulichkeitsvereinbarungen
- Verschlüsselung von E-Mails
- Formulieren und Durchsetzen der Passwortrichtlinien
- Fernlöschung von dienstlichen Daten, z.B. am Smartphone oder Tablet
- VPN-Verbindungen
- Datensicherung
- Ausschließlicher Einsatz einer hauseigenen Cloud-Lösung

Welche Maßnahmen muss ich gemäß § 6 Datenschutzgesetz setzen?

- Grundsätzlich sind alle Informationen und Daten, die Ihnen im Rahmen Ihrer Tätigkeit anvertraut oder zugänglich gemacht worden sind, geheim zu halten (Datengeheimnis) — es sei denn, es gibt einen rechtlich zulässigen Grund für deren Weitergabe („Übermittlung“).
- Eine solche Weitergabe durch Sie darf nur erfolgen, wenn Sie dazu von der DGS ausdrücklich ermächtigt wurden — die Weitergabe muss Ihnen gegenüber angeordnet worden sein.
- Selbstverständlich darf diese Anordnung nicht rechtswidrig sein — Sie müssen und dürfen sie in solch einem Fall nicht befolgen und dürfen arbeitsrechtlich deswegen auch nicht belangt werden.
- Eine Verpflichtungserklärung zu § 6 Datenschutzgesetz muss von Ihnen unterschrieben worden sein.

Im Zweifel sind Daten und Informationen vertraulich zu behandeln.
Interne Rückfragen sind kein Zeichen von Schwäche. Sie befolgen lediglich das Gesetz.

Beispiele: keine lautstarken Unterhaltungen über DGS-Interna in öffentlichen Verkehrsmitteln; keine Gespräche über vertrauliche Aspekte dienstlicher Arbeit bei einem Abendessen; keine Erstellung von Gratulationslisten ohne vorherige rechtsgültige Einwilligung; keine private Verwendung dienstlicher Daten wie z.B. das Abfragen von Daten über Bekannte.

Tipps zum Umgang mit Besucher/inne/n

- Holen Sie Ihre Gäste oder Lieferant/inn/en beim Eingang/Sekretariat ab — idealerweise betreten Besucher/innen die geschützten Bereiche erst mit Ihnen gemeinsam.
- Lassen Sie Ihre Besucher/innen nicht alleine durch die Räumlichkeiten gehen — begleiten Sie sie auch wieder aus den geschützten Bereichen hinaus.
- Erinnern Sie Kolleg/inn/en daran, Besucher/innen hinauszubegleiten, wenn die Besucher/innen von Ihnen nur zu Ihren Kollegen/innen gebracht worden sind.
- Treffen Sie Besucher/innen vorzugsweise in Besprechungsräumen und nicht in Ihren Büros — es könnten dort vertrauliche Informationen einsehbar sein. z.B. freiliegende Dokumente.
- Denken Sie daran, dass auf Flipcharts und auf Notizen an den Wänden vertrauliche Informationen stehen können. Es dauert nur Sekunden, um sie mit einem Smartphone abzufotografieren — entsorgen sie daher Flipchart-Blätter durch Zerreißen und verzichten Sie darauf, vertrauliche Informationen an den Wänden, vor allem längerfristig, aufzuhängen.
- Sprechen Sie scheinbar herumirrende Personen an, fragen Sie, wohin sie möchten und begleiten Sie sie — seien Sie selbstbewusst und lassen Sie sich nicht abwimmeln.

Was muss ich tun, damit Unterlagen und elektronische Datenträger sicher entsorgt werden können?

- Verwenden Sie für interne und vertrauliche Unterlagen auf Papier, soweit vorhanden, Datenschutzcontainer und Shredder — und entsorgen Sie auf diesem Weg lieber einmal ein Dokument zu viel als zu wenig.
- Haben Sie weder einen Datenschutzcontainer noch einen Shredder zur Verfügung, z.B. auf Reisen, dann nehmen Sie die Unterlagen wieder in Ihr Büro mit und vernichten Sie sie dort.
- Bewerbungsunterlagen sind nach Gebrauch vollständig an die organisatorisch zuständige Stelle, in der Regel an das Personalbüro, zu übergeben.
- Bringen Sie elektronische Datenträger wie USB-Sticks, CDs, DVDs etc. mit internen oder vertraulichen Daten zur IT-Abteilung zur fachgerechten Vernichtung und Entsorgung.
- Erreichen Ihre dienstlichen IT-Endgeräte das Ende ihrer Nutzungsdauer oder sind defekt, retournieren Sie diese an die IT-Abteilung.

Beachten Sie bitte auch
die „Informationssicherheitsrichtlinie der Diözese Graz-Seckau und ihrer Einrichtungen“

Was muss ich in Bezug auf Datensicherung beachten?

- Daten auf zentralen Systemen werden von der IT-Abteilung routinemäßig gesichert.
- Speichern Sie Ihre Daten daher ausschließlich auf Ihrem persönlichen zentralen Speicherbereich oder an anderen, zentral gesicherten Speicherorten.

Sichern Sie dienstliche Daten, insbesondere schützenswerte, auf keinen Fall auf unverschlüsselten mobilen Datenträgern, z.B. auf USB-Sticks, Speicherkarten oder externen Festplatten oder auf der lokalen Festplatte Ihres Desktops, Notebooks oder Tablet PCs.

Was muss ich bei der E-Mail-Nutzung beachten?

- Die DGS erlaubt **keine** private Nutzung dienstlicher E-Mail-Adressen.
- Nach österreichischer Rechtslage dürfen E-Mails an mehr als 50 E-Mail-Empfänger/innen zu Aussendungs- und Werbezwecken nur dann versendet werden, wenn vorher deren Zustimmung eingeholt worden ist.

Hilfreiche Tipps zum Schutz vor Betrug im Zusammenhang mit E-Mail finden Sie z.B. auch auf der Watchlist Internet.

Weitere, durchaus wichtige Informationen zu Massenmailings finden Sie bei der WKO.

Was muss ich bei der Internet-Nutzung beachten?

- Die DGS erlaubt Ihnen eine eingeschränkte private Nutzung Ihres Internet-Zugangs. Alle untenstehenden Regelungen beziehen sich auf beide Formen der Nutzung: dienstlich und privat.
- Seien Sie sich bewusst, dass über die so genannte IP-Adresse jeder Zugriff in das Internet auf die DGS verweist, Sie also indirekt auch immer im Namen der DGS agieren.
- Urheber- und Markenrechte sind zu wahren und Lizenzbestimmungen sind einzuhalten.
- Bedenken Sie, dass die private Internet-Nutzung insbesondere rechtlich eine Vielzahl von Fragen aufwirft und reduzieren Sie sie bitte auf ein Minimum.

Hilfreiche Tipps zum Schutz vor Online-Betrug und vor Fallen finden Sie z.B. auch auf der Watchlist Internet.

Wie mache ich meinen Arbeitsplatz sicherer?

- Stellen Sie sicher, dass in Ihrem Arbeitsbereich Unterlagen und Datenträger, z.B. USB-Sticks, mit internen oder vertraulichen Informationen nicht durch Unberechtigte einsehbar abgelegt sind — räumen Sie interne und vertrauliche Unterlagen, jegliche Datenträger sowie mobile IT-Endgeräte bei Abwesenheit in einen Kasten oder eine Lade und versperren Sie diese, sofern möglich.
- Sollte z.B. Reinigungspersonal Ihren Arbeitsbereich üblicherweise unbeaufsichtigt betreten können, müssen Sie zu diesen Zeiten schutzbedürftige Unterlagen, Datenträger und IT-Endgeräte auf jeden Fall zugangsgeschützt lagern.
- "Sperren" Sie Ihren PC bzw. ihr Notebook, sowohl wenn Sie Ihren Arbeitsplatz kurzfristig, besonders aber für längere Zeit verlassen, mit der Tastenkombination **Windows-Taste+L** und lassen Sie Smartphones, Tablet oder Tablet PCs etc. nicht unversperrt, d.h. ohne PIN bzw. Passwort im Raum liegen.
- Beachten Sie auch die „Informationssicherheitsrichtlinie der Diözese Graz-Seckau und ihrer Einrichtungen“.

Denken Sie daran, dass Sie gemäß DSGVO und Datenschutzgesetz verpflichtet sind, Unterlagen und Datenträger vor unberechtigtem Zugriff zu schützen. Das betrifft auch Notebooks, Smartphones, Tablets etc., die häufig von Betriebsfremden, manchmal leider aber auch „Insidern“, gestohlen werden.

Die Rolle von Führungskräften

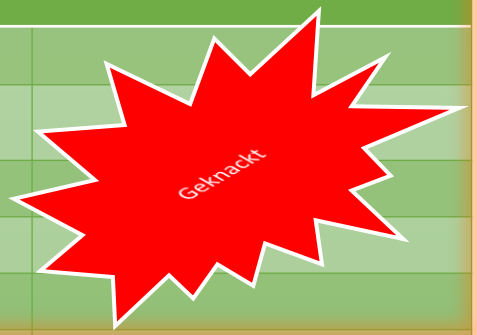
Führungskräfte

- sind ihren Mitarbeiter/inne/n gegenüber ein Vorbild in der Einhaltung der Regeln, Prozesse und gesetzlichen Vorgaben
- stehen ihren Mitarbeiter/inne/n für Rücksprachen zur Verfügung
- informieren ihre Mitarbeiter/inne/n, dass sie bei Bekanntwerden sicherheitsrelevanter Vorfälle unverzüglich zu informieren sind
- melden sicherheitsrelevante Vorfälle, insbesondere solche mit möglicher Öffentlichkeitswirksamkeit, unverzüglich dem Datenschutzzuständigen Ihrer Einrichtung
- fördern eine gute Kultur im Umgang mit Daten und IT durch regelmäßige Erwähnung der Themen Informations- und Datenschutz und der damit verbundenen Anforderungen
- ermutigen ihre Mitarbeiter/innen, im Zweifel rückzufragen und Entscheidungen, wie z.B. Datenweitergaben, nicht vorschnell und alleine zu treffen
- sprechen die Bedeutung von Datenschutz für die DGS immer wieder an, auf jeden Fall aber bei Mitarbeiter/innen/gesprächen
- fordern von ihren Mitarbeiter/inne/n laufend die Einhaltung der Regeln, Prozesse und gesetzlichen Vorgaben ein und setzen Schulungsmaßnahmen wirksam um

„Knackdauer“ bei Passwörtern

Rechengeschwindigkeit des Computers: rund zwei Milliarden Varianten pro Sekunde

Passwortlänge	„Knackdauer“	Einheit	Anmerkung
a-z, A-Z, 0-9 (= 3 Merkmale)	maximal		
6	27	Sekunden	
7	28	Minuten	
8	29	Stunden	
9	75	Tage	
10	12	Jahre	
11	**787**	**Jahre**	
12	**48.804**	**Jahre**	
13	**3.025.880**	**Jahre**	**> 3 Millionen Jahre**
14	**187.604.571**	**Jahre**	**> 187 Millionen Jahre**
15	**11.631.483.455**	**Jahre**	**> 11 Milliarden Jahre**



„Tipps“ für de facto wirkungslose Passwörter

In der Praxis unsichere Passwörter sind

- kurz, z.B. weniger als 10 bis 12 Zeichen lang – außer es sind PINs, wie z.B. auf SIM-Karten, die nach wenigen Fehlversuchen gesperrt werden
- einfache Wörter und Namen, z.B. Bärchen, Passwort, Fritz, Laura
- schlicht aufgebaut, z.B. 0000, 123456, abcfeghi, qwertzuio (Tasten nebeneinander)
- ident mit Wörtern aus Wörterbüchern
- etc.

Erfolgreiches „Passwort-cracken“ ist damit ein Kinderspiel.

Wie aber sehen wirksame Passwörter aus?

Tipps für sichere, recht leicht merkbare Passwörter

- Erzeugen Sie lange Passwörter und ändern Sie diese regelmäßig — das macht alles einfacher:
  8 Zeichen sind das Minimum, 12 bis 16 Zeichen sind empfehlenswert.
- Denken Sie bildlich.
- Verwenden Sie Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen:
  Bin1Schon2Hier3 — &waa7ruum? — DerWurmIm%Sturm
- Reihen Sie Wörter aneinander oder teilen Sie sie:
  2Und2istVier? — Uff!Zack!Knuff! — Per1Se2Polis
- Reimen Sie:
  3Motten&5Karotten — Elch&Kelch5 — Heuteister!beute! — EinBIER-um4
- Verwenden Sie Dreiergruppen aus Buchstaben in Kombination mit Ziffern, das ist eingängiger:
  &Aaa4Bee5Cee — Nic9Jul8Ras7
- Warum nicht Dialekt?
  Schneeisschee! — 17IsaguatsJoa — A.quartal.isaQual — MeiPWIsASchee

Schlechter Umgang mit Passwörtern sieht so aus

Passwörter werden beispielsweise leichtfertigerweise

- auf Zetteln gut zugänglich notiert
- auf PCs, Notebooks, Smartphones etc. unverschlüsselt gespeichert
- mit anderen geteilt
- vor anderen mitlesbar eingeben
- sehr selten oder nie geändert
- ident bei verschiedenen Diensten genutzt („eines für alles“)
- über E-Mail verschickt
- im Browser abgespeichert
- auf fragwürdigen Seiten oder in zweifelhafte Apps eingegeben

Identitätsdiebstahl steht nun nichts mehr im Weg.

Wie aber sieht guter Umgang mit Passwörtern aus?

Vernünftiger Umgang mit Passwörtern hingegen sieht folgendermaßen aus

Passwörter — dienstliche, sinnvollerweise aber auch private — werden

- geheim gehalten — das gilt zwingend gegenüber allen Personen, auch Familienmitgliedern und Partnern
- wenn überhaupt, nur an schwer zugänglichen, anderen Personen unbekannten Orten notiert
- auf PCs, Notebooks, Smartphones etc. nur verschlüsselt gespeichert — im Zweifel allerdings überhaupt nicht
- geändert, wenn andere sie gesehen haben oder kennen könnten
- regelmäßig geändert, und sei es auch nach längerer Zeit
- niemals bei anderen Diensten wiederholt genutzt („eines pro Dienst“)
- nie über E-Mail verschickt
- nie im Browser abgespeichert
- nie auf fragwürdigen Seiten oder in zweifelhafte Apps eingegeben

Was ist Phishing und wie schütze ich mich davor?

- Phishing ist ein Variante des „Social Engineering“, der zwischenmenschlichen Beeinflussung für unlautere Zwecke — hier oft für Identitätsdiebstahl.
- Misstrauen Sie dringend erscheinenden E-Mails, die von Ihnen unter Zeitdruck persönliche Daten und/oder Zugangsdaten, auch PINs und TANs abfragen möchten, z.B. indem Ihnen mit der Sperre von Zugängen gedroht wird.
- Reagieren Sie nicht auf E-Mails, in denen, unter welchem Vorwand auch immer, auf verlinkten Webseiten die Eingabe von Zugangsdaten gefordert wird. Dasselbe gilt auch für Apps, die angeblich aufhören zu funktionieren, wenn Sie nicht einen speziellen Link anklicken.
- Geben Sie Zugangsdaten nie über unsichere Internetverbindungen ein, d.h. keinesfalls über „http“-Webseiten, sondern nur über solche, die mit „https“ beginnen.
- Auch betreffend Telefonie gilt: Übermitteln Sie keine vertraulichen Daten (Benutzernamen, Passwörter, TANs etc.), ausgenommen wenn Sie sicher, dass der/die Empfängerin vertrauenswürdig ist. Ein Beispiel: Sie haben Ihre Bank oder Ihren Internet-Provider selbst unter der Ihnen bekannten Service-Telefonnummer angerufen: Dann ist das die sicherste Form der Kontaktherstellung.

Weitere Praxistipps zum Schutz vor Passwort-Phishing finden Sie z.B. auf der Watchlist Internet und im "IT-Sicherheitshandbuch für Mitarbeiter/innen" der WKO ab Seite 26.

Was ist „Ransomware“ (Erpressungs-Software)?

- Erpressungstrojaner sind eine besondere Form von Schadsoftware, d.h. von Computerprogrammen, die vorsätzlich schädigende Funktionen auszuführen. Der Begriff bezeichnet also keine schadhafte, sondern gewollt schädigende Software.
- Erpressungstrojaner, auch Lösegeldtrojaner, Verschlüsselungstrojaner und „Ransomware“ (Erpressungs-Software) genannt, verschlüsseln in der Regel alle Dokumente, Tabellen, Präsentationen, Fotos, Musikdateien und sonstigen Nutzerdaten, zu denen diese Software Zugang erlangt. Gegen Bezahlung eines Lösegelds an die organisierte Kriminalität werden diese Dateien – zumeist – wieder entschlüsselt.
- Eintrittswege für diese Form der Schadsoftware sind in der Regel
- E-Mail-Anhänge, z.B. scheinbare Rechnungen, Paketankündigungen oder Bewerbungen und
  - von den Kriminellen verseuchte oder präparierte Webseiten, die Sicherheitsschwachstellen auf schlecht gepflegten IT-Systemen der Nutzer ausnützen.
  - Der wesentlichste Schutz vor derartiger Erpressung ist das Sichern von Daten auf den zentral gesicherten Speicherbereichen der DGS und der vorsichtige Umgang mit erhaltenen Dateien, z.B. Dokumenten und Tabellen.
- Leisten Sie keinesfalls Zahlungen.

Für Details und aktuelle Beispiele von im Umlauf befindlichen Erpressungstrojanern und für Schutzmaßnahmen und Tipps werfen Sie bitte einen Blick auf die äußerst hilfreiche Seite der Watchlist Internet.

Was ist Schadsoftware und wie schütze ich mich davor?

- Schadsoftware bezeichnet Computerprogramme, die vorsätzlich schädigende Funktionen auszuführen.
- Der Begriff bezeichnet also keine schadhafte, sondern gewollt schädigende Software.
- Das kann z.B. das Löschen von Dateien sein, das Verschlüsseln von Daten und Erzwingen von Lösegeldzahlungen oder das Einnisten von Software zum Zweck des Ausspähens von Tastaturanschlägen, z.B. bei der Passworteingabe.

Sie als Mitarbeiter/in haben es in der Hand, jene Angriffe abzuwehren, die technisch nicht verhinderbar sind:

- Sichern sie wichtige Daten auf zentrale Systeme.
- Misstrauen Sie E-Mails und Anhängen, insbesonders unbekannten Ursprungs und fragen Sie bei Unsicherheit beim Absender nach, bevor Sie die Datei im Anhang öffnen.

Für Details und aktuelle Beispiele von im Umlauf befindlicher Schadsoftware und für Schutzmaßnahmen werfen Sie bitte einen Blick auf die Seite der Watchlist Internet.

Was ist Social Engineering?

- Social Engineering ist die Kunst, Menschen dahingehend zu beeinflussen, dass sie bestimmte Verhaltensweisen setzen, selbst wenn diese nicht in ihrem Interesse liegen. Z.B. könnte sich jemand Zutritt zu einem Gebäude verschaffen, indem er, gut gekleidet und selbstbewusst, eine sich schließende Tür noch schnell aufdrückt und sich, dem vor ihm Eingetretenen dankend, zügig Zutritt zu einem Bereich verschafft, der eigentlich nur Personen mit Zutrittskarte offensteht.
- Social Engineering stellt einen Angriff auf menschliches Verhalten dar und kann als eine Form von Hacking gesehen werden.
- Die Schwachstelle bei Social Engineering ist der Mensch, nicht die Technik.
- In der Regel dient Social Engineering missbräuchlichen Zwecken wie Daten- und Identitätsdiebstahl, Spionage und Betrug.
- Zu den Methoden von Social Engineering gehören gezieltes Aushorchen von Mitarbeiter/inne/n, widerrechtliches Abfragen oder Abfangen von Passwörtern, das unerlaubte Erwirken von Zutritt zu Gebäuden und Büros etc.
- Angreifer spionieren das persönliche Umfeld ihres Opfers aus, spiegeln falsche Identitäten vor oder nutzen Schwächen wie Autoritätshörigkeit.
- Es wird tief in die Trickkiste der Psychologie gegriffen, per Telefon, Brief, Fax, E-Mail, über Social Media, persönliches Ansprechen und viele weitere Wege.

Praxistipps zum Schutz vor Social Engineering über E-Mail, Fax und am Arbeitsplatz

Sie bekommen ein E-Mail oder Fax, das Sie unsicher macht oder begegnen im Bürobereich jemanden, der etwas zu suchen scheint, ziellos wirkt oder sogar ganz besonders forsch auftritt?

Seien Sie selbstbewusst und bestimmt.
Sie tun damit genau das Richtige.

- Lassen Sie sich nicht unter Druck setzen, versuchen Sie, Zeit zu gewinnen — sagen Sie „Lassen Sie uns zum Sekretariat gehen“ oder sprechen Sie mit Kollegen über das seltsame E-Mail, das Sie gerade erhalten haben.
- Begleiten Sie Personen, die behaupten sich verlaufen zu haben, zum Ausgang.
- Seien Sie hilfsbereit — und dennoch vorsichtig. Hier liegt Ihre größte Schwachstelle.
- Geben Sie beim leisesten Zweifel oder kleinstem unangenehmen Gefühl keinerlei Informationen oder personenbezogene Daten preis — weder über sich noch über andere.
- Tätigen Sie größere Zahlungen, sofern dies zu Ihren dienstlichen Aufgaben gehört, nur nach dem Vier-Augen-Prinzip.
- Melden Sie Ungewöhnliches lieber einmal zu viel als zu wenig — und dies rasch.

Praxistipps zum Schutz vor Social Engineering über Telefon und im Gespräch

Sie bekommen einen Anruf oder werden persönlich angesprochen? Man will Auskünfte, ist seltsam neugierig oder schmeichelt Ihnen? Sie fühlen sich daher unwohl?

Seien Sie zurückhaltend und fragen Sie zurück.
Sie tun damit genau das Richtige.

- Lassen Sie sich nicht unter Druck setzen, versuchen Sie, Zeit zu gewinnen — sagen Sie „Moment bitte, es läutet gerade“ oder „Moment, ich bin gleich wieder bei Ihnen“.
- Fragen Sie zurück und bitten Sie um Kontaktdaten. Sagen Sie beispielsweise, Sie seien nicht zuständig und benötigten daher diese Daten.
- Bitten Sie am Telefon freundlich um eine Rückrufnummer. Sagen Sie, Sie müssten dies tun und halten Sie nach dem Gespräch rasch Rücksprache mit Ihrem Vorgesetzten oder melden Sie den Vorfall.
- Bei (angeblichen) Anrufen durch die Presse sagen Sie, sie seien nicht auskunftsberechtigt und verweisen Sie an die Pressestelle. Verständigen Sie ehestmöglich die von Ihnen genannte Stelle über allfällige Bedenken Ihrerseits.
- Melden Sie ungewöhnliche Anrufe und Gespräche lieber einmal zu viel als zu wenig.

Was im Zuge der Social Media-Nutzung so alles schief gehen kann — Beispiele

Im Zuge der Nutzung von Social Media kann leider vieles daneben gehen:

- Schadsoftware gelangt in das Netzwerk der DGS, z.B. über eine der unzähligen Social Media Software-Schwachstellen
- Äußerungen lassen Rückschlüsse auf innerbetriebliche Aktivitäten zu, z.B. über geplante organisatorische Änderungen, das Betriebsklima und Schwachstellen in der DGS
- Es entstehen Gerüchte
- Geschäftsgeheimnisse werden publik
- Der Ruf der DGS wird geschädigt
- Es kommt zu Urheberrechtsverstößen
- Es kommt zu Datenschutzverletzungen
- Es wird unbewusst eine Informationsbasis geschaffen, die für Social Engineering missbraucht werden kann — denn Daten sind das Öl des 21. Jahrhunderts

Wenn ich Social Media nutze — worauf muss ich achten?

Wenn Sie Social Media-Plattformen und -Werkzeuge, z.B. integrierte Kommunikationskanäle, nutzen, damit also vorwiegend öffentlich agieren, achten Sie besonders auf die folgenden Punkte:

- Wesentliche Aspekte sind in der „Informationssicherheitsrichtlinie der Diözese Graz-Seckau und ihrer Einrichtungen“ geregelt.
- Interne und vertrauliche Daten und Informationen dürfen über Social Media-Plattformen nicht kommuniziert werden.
- Social Media-Plattformen und -Werkzeuge sind meist nichts anderes als öffentliche Cloud-Lösungen. Berücksichtigen Sie daher die „Informationssicherheitsrichtlinie der Diözese Graz-Seckau und ihrer Einrichtungen“.
- Achten Sie auf die komplexe Problematik des Urheberrechts und des Markenrechts. Besonders bei Bildern ist größte Vorsicht geboten, wenn diese nicht von der DGS selbst bereitgestellt worden sind.
- Selbstverständlich sind keinerlei geschäfts- oder kreditschädigende oder persönliche Äußerungen über dienstliche Gegebenheiten zulässig.

Seien Sie sich bewusst, dass über die so genannte IP-Adresse jeder Zugriff auf Social Media-Plattformen, der aus dem Netzwerk der DGS heraus erfolgt, nachvollziehbar ist.

Die Nutzung von Social Media erfordert Sparsamkeit bei der Preisgabe von Daten und Informationen und setzt sowohl eigenverantwortliches Handeln als auch Hausverstand voraus.

Wie verhalte ich mich in der Öffentlichkeit, um interne und vertrauliche Informationen zu schützen?

- Führen Sie keine vertraulichen Gespräche mit dienstlichen Inhalten beispielsweise in öffentlichen Verkehrsmitteln wie Bussen, Straßenbahnen oder Flugzeugen, am Mittagstisch in Restaurants, bei externen Veranstaltungen etc., außer Sie haben sich vorab überzeugt, dass niemand Unbefugter Sie hören oder Unterlagen einsehen kann. Das gilt auch für Telefonate.
- Benützen Sie ein Notebook, Tablet oder Smartphone nur dann, wenn Sie sich überzeugt haben, dass niemand Unbefugter Ihren Bildschirm einsehen kann.
- Stellen Sie die Dauer für die Aktivierung der Gerätesperre so kurz wie möglich ein, z.B. am Smartphone auf eine oder zwei Minuten und auf Aktivierung beim Drücken des Ein-Ausschalters.
- In Flugzeugen, je nach Sitzanordnung auch in der Bahn, sollten Sie Notebooks nicht verwenden, da es so gut wie immer Menschen gibt, die mitlesen können. Dort hilft selbst eine spezielle Datenschutzfolie, die seitliches Mitlesen verhindert, nur selten.
- Vermeiden Sie, wann immer möglich, die Erwähnung von Nachnamen von Personen und Namen von Firmen, Behörden, Einrichtungen etc.

Tipps für unterwegs — z.B. im Auto, im Bus, in der Bahn und Straßenbahn

- Was nicht mitgenommen wird, kann nicht gestohlen werden oder verloren gehen
- Muss Papier wirklich mit, wenn es vertrauliche Daten enthält?
- USB-Sticks nur mitnehmen, wenn vertrauliche Daten darauf verschlüsselt sind.
- Das Auto ist kein Safe — Geräte, Taschen etc. darin nie sichtbar liegen lassen.
- Geräte wie Smartphones, Tablets und Notebooks nie unbeaufsichtigt liegen lassen, nicht im Meetingraum, nicht im Lokal, nicht für einen Toilettenbesuch.
- Wertsachen, also auch Smartphones und Tablets, nicht mit Kleingepäck, v.a. nicht in Außentaschen, aufgeben.
- Zugangsdaten nie auf fragwürdigen Geräten eingeben, etwa auf fremden Privatgeräten, auf Hotelgeräten oder in Internet-Cafés.

Was tue ich bei Sicherheitsvorfällen und wenn ich Sicherheitsmängel vermute oder entdecke?

Zögern Sie bitte nicht, Vorfälle oder Mängel zu melden: Es geht der DGS nicht darum, Schuldfragen zu klären, sondern Schäden durch Sicherheitsvorfälle und -mängel zu minimieren und zukünftig auszuschließen.

Meldung von sicherheitsrelevanten Vorfällen oder Sicherheitsmängeln:

- An Ihren Vorgesetzten. Dieser entscheidet, ob er mit dem Datenschutzzuständigen oder auch dem IT-Verantwortlichen Kontakt aufnimmt.

Löschen Sie nach der Meldung weder E-Mails noch andere Daten und verwenden Sie die betroffenen Geräte nicht weiter.

Eine Pflicht zur **umgehenden** Meldung besteht beispielsweise

- bei Verlust oder Diebstahl von Unterlagen oder von IT-Endgeräten, z.B. von Smartphones, Tablets oder Notebooks
- bei ungewöhnlichen E-Mails oder Anrufen, insbesondere, wenn dabei nach Passwörtern oder Informationen über Kollegen gefragt wird
- bei Auftreten von ungewollter Datenverschlüsselung, verbunden mit Zahlungsaufforderungen — sogenannten Erpressungstrojanern
- bei irrtümlichem Versand von z.B. E-Mails mit vertraulichem Inhalt
- bei Bekanntwerden, dass vertrauliche Daten unrechtmäßig an die Öffentlichkeit gelangt sind

Melden Sie sicherheitsrelevante Vorfälle und Sicherheitsmängel im Zusammenhang mit IT umgehend — große Schäden in anderen Organisationen hätten verhindert werden können, wären Vorfälle oder Auffälligkeiten rasch gemeldet worden.

Aktuell geltende Regelungen und Empfehlungen

- Datenschutz-Grundverordnung (DSGVO)
- Datenschutzgesetz (DSG 2018)
- Decretum Generale über den Datenschutz in der Katholischen Kirche in Österreich und ihren Einrichtungen (kirchliche Datenschutzverordnung)
- Datenschutzrichtlinie der Katholischen Kirche Österreich
- „Informationssicherheitsrichtlinie der Diözese Graz-Seckau und ihrer Einrichtungen“

Externe Sicherheitstipps finden Sie z.B. hier:

- IT-Sicherheitshandbuch für Mitarbeiter/innen (WKO)
- IT-Sicherheitshandbuch für leitende Mitarbeiter/innen (Führungskräfte) (WKO)