Die kleine

DATENSCHUTZFIBEL

Wichtiges zu Datenschutz und IT-Sicherheit

Für Mitarbeitende und Ehrenamtliche des
Pommerschen Evangelischen Kirchenkreises

Pommerscher
Evangelischer Kirchenkreis

DIE KLEINE DATENSCHUTZFIBEL

INHALT

I. PRAXISTIPPS FÜR DEN DATENSCHUTZ- UND IT-ALLTAG

PASSWÖRTER

Nutzen Sie grundsätzlich Passwörter! Vor allem durch Passwörter, aber auch z.B. durch USB-Schlüssel, ist Dritten der Zugang zum PC oder zum Smartphone verwehrt. Sofern das Programm keine abweichenden Vorgaben gegeben hat, gehen Sie bei der Vergabe Ihrer Passwörter wie folgt vor:

Denken Sie sich ein Passwort aus, das alle nachfolgenden Kategorien enthält

- 2 Großbuchstaben
- 2 Kleinbuchstaben
- 1 Sonderzeichen
- 2 Ziffern
- mindestens 10 Zeichen

Vermeiden Sie Passwörter, die durch Dritte leicht zu erraten sind (wie z.B. Vor- und Familiennamen, Geburtstage oder trivial angeordnet Zahlenkombinationen wie 12345678).

TIPP:

Denken Sie sich einen Satz mit einem Geschehnis aus Ihrem tatsächlichen Leben aus, der Großschreibung, Sonderzeichen und Zahlen enthält. Nehmen Sie von den Worten dieses Satzes jeweils den ersten Buchstaben

Beispiel: Der Passwortsatz „Meine Sneaker habe ich 50 % günstiger bekommen" ergibt das Passwort „MShi50%gb"

WICHTIG:

Verwenden Sie für unterschiedliche Anwendungen unterschiedliche Passwörter.

Im Internet ist dies eine wichtige Sicherheitsvorkehrung, falls bei einem Internetanbieter, bei dem Sie Kunde sind, Ihr Passwort und Ihre Mailadresse gehackt worden sind.

Nur so sind die Anmeldungen bei anderen Anbietern davon nicht betroffen, auch wenn Sie dieselbe Mailadresse angegeben haben.

SICHERE VERWAHRUNG VON PASSWORTEN

- Passworte sind stets geheim zu halten!
- Behalten Sie Passwörter am Besten im Kopf!
- Passwortlisten in Papierform gehören in den Tresor.
- Passwörter niemals speichern!
- hilfreich ist das Passwort-Merkblatt des BSI

  https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Checklisten/studie-accountschutz-passwort-merkblatt.pdf?__blob=publicationFile&v=4

NUTZUNG VON E-MAIL

Prüfen Sie vor dem Versand einer E-Mail, dass der Adressat der E-Mail

1. auch der Berechtigte zum Empfang der enthaltenen Information ist

2. die Mailadresse des Adressaten richtig ist und Sie bei der Eingabe oder Auswahl nicht versehentlich der Autokorrektur oder einem falschen Vorschlagsfeld auf den Leim gegangen sind.

VERSAND AN MEHRERE EMPFÄNGER

Soll die E-Mail an eine Vielzahl von Empfängern verschickt werden, ist es wichtig, die Felder CC: (auch „Kopie“) und BCC: (auch „Blind-kopie“) korrekt zu verwenden.

Das CC:-Feld ist für Empfänger gedacht, die Kenntnis vom Inhalt haben sollen, ohne selbst aktiv werden zu müssen, und die erfahren sollen, welcher Empfängerkreis die Mail erhalten hat.

Das BCC:-Feld ist für Empfänger gedacht, für die es keinen Anlass gibt, voneinander zu erfahren, wie z.B. bei Newslettern. Dies ist aus Datenschutzgründen sehr wichtig!

Prüfen Sie zunächst, ob das BCC:-Feld im Adressfeld Ihres Mail-programms angezeigt wird. Andernfalls richten Sie es dauerhaft ein. Vor dem Versand an mehrere Empfänger ist zu prüfen, ob diese notwendigerweise die Information erhalten müssen.

Bei Problemen oder Fragen wenden Sie sich an ihre zuständige IT-Abteilung.

VERSCHLÜSSELTER VERSAND VON DATEIANHÄNGEN

Wenn Sie Dokumente mit sensiblen Daten per E-Mail versenden, sollten diese im Zweifel als verschlüsselter Dateianhang versendet werden.

Halten Sie sich hierbei an die bestehenden Vorgaben, wie die Verschlüsselung vorgenommen werden soll (z.B. 7zip)

Teilen Sie dem Empfänger das Kennwort telefonisch oder per SMS mit, auf keinen Fall jedoch durch eine weitere E-Mail!

ANHÄNGE UND LINKS EINGEHENDER MAILS

Besondere Vorsicht ist angesagt bei allen eingehenden Mails mit Anhängen.

- Haben Sie ein E-Mail von einer Ihnen unbekannten Mailadresse erhalten?
- Oder kennen Sie den Absender, erwarten aber kein Mail?

Selbst wenn Sie den Absender kennen:

- Öffnen Sie auf keinen Fall den Anhang der Mail oder den in der Mail genannten Link!
- Klären Sie zunächst mit dem Absender, ob dieser tatsächlich der Urheber der Mail ist.

DENN:

Durch künstliche Intelligenz oder das sogenannte Social-Engineering ist es für Internetkriminelle möglich, Verbindungen zwischen Personen nachzuvollziehen und dies mit einer gefälschten Mail, die im Anhang oder im Link Schadsoftware enthält, auszunutzen.
Wenden Sie sich bei Fragen unbedingt an ihre IT-Abteilung.

Achten Sie auf Ihren Virenscanner!

Besteht der Verdacht auf Virenbefall, sind umgehend alle Arbeiten einzustellen und die IT-Betreuung ist einzuschalten.

BEACHTEN SIE IN DIESEM FALL DIE HINWEISE AUF DER RÜCKSEITE DIESER FIBEL!

CLEAN-DESK-POLICY („GRUNDSATZ DES SAUBEREN SCHREIBTISCHS“)

Sichern Sie Ihren Arbeitsplatz immer vor Einsichtnahme oder dem Zugang Dritter zu personenbezogenen Daten:

Achten Sie darauf, dass auf Ihrem Schreibtisch und ihrem PC-Bildschirm nur Akten offen bzw. Dateien sichtbar sind, die Sie aktuell für die Bearbeitung benötigen.

Handelt es sich dabei um Dokumente mit personenbezogenen Daten, sollte davon keine andere Person Kenntnis nehmen können.

Wenn Sie Ihren Arbeitsplatz verlassen oder wenn Besucher den Raum betreten, schließen Sie alle offenen Akten und sperren Sie Ihren PC-Bildschirm, bzw. positionieren Sie die Person so, dass sie keine Einsicht nehmen kann.

Überprüfen Sie Ihren Schreibtisch daraufhin, ob interessante schriftliche Notizen lesbar sind (Post-it® Haftnotizen, beschriebene Schreibunterlage usw.), die Sie besser vor der Kenntnisnahme Dritter schützen sollten.

VERLASSEN DES ARBEITSPLATZES

Aktivieren Sie beim Verlassen Ihres Windows PCs oder Laptops die Desktopsperre mit dem Tastenkürzel

oder Strg + Alt + Entf!

Fahren Sie am Arbeitsende Ihren PC herunter, räumen Sie Ihren Schreibtisch auf und offenliegende Akten weg. Schließen Sie Fenster und Türen.

TELEFON

Bevor Sie am Telefon Auskünfte geben, vergewissern Sie sich, dass die Person am Telefon auch wirklich diejenige Person ist, für die sie sich ausgibt.

Sollten Sie Zweifel an der Identität der Person haben, verschicken Sie die gewünschte Information per Post an die in der Verwaltung hinterlegte Anschrift oder Mailadresse.

Nehmen Sie in diesem Fall keine neue Anschrift oder Mailadresse zum Versand der Informationen entgegen, dies könnte ein Trick sein.

Senken Sie die Lautstärke beim Telefonieren, wenn sich Besucher in Ihrer Nähe befinden.

BESUCHER

Wenn Sie einen Besucher im Büro empfangen, achten Sie darauf, Telefonate und Akten vor dem Besucher geheim zu halten und ihn in den Räumen nicht allein zu lassen.

COMPUTER-FERNWARTUNG

Bevor Sie einem Service-Techniker den Zugriff auf Ihrem Computer per Fernwartung erlauben, vergewissern Sie sich, dass die Person tatsächlich dazu berechtigt ist.

Bevor Sie die Zugriffserlaubnis erteilen, schließen Sie alle für den Service-Techniker nicht relevanten Programme. Bleiben Sie während der gesamten Fernwartung am PC.

VIRENSCHUTZ

Stellen Sie sicher, dass nur 1 Antivirenprogramm auf dem PC installiert ist, und dass dieses auf dem PC eingeschaltet und aktuell ist.

Installieren Sie Software-Updates zeitnah oder wenden Sie sich an Ihre IT- Abteilung.

Versichern Sie sich regelmäßig bei Ihrem IT-Administrator, dass die Funktionstüchtigkeit der Sicherheitssysteme regelmäßig überprüft bzw. aktualisiert wird.

DATENSICHERUNG DIGITAL UND ANALOG

Legen Sie alle personenbezogenen Dateien im Verwaltungs-programm oder in Dateiordnern ab, von denen Sie wissen, dass sie durch eine Datensicherung regelmäßig gesichert werden.

Aktenordner mit vertraulichen personenbezogenen Informationen, wie zum Beispiel Personalordner, sind in verschlossenen Schränken zu verwahren.

PLANMÄSSIGE VERNICHTUNG VON DATENSPEICHERN UND AKTENORDNERN

Stellen Sie sicher, dass Datenträger und Aktenordner von einer Spezialfirma unwiederbringlich und datenschutzkonform vernichtet werden.

Wird ein Drucker oder ein Kopierer ausgetauscht, achten Sie darauf, dass Ihnen die Festplatten ausgehändigt werden. Alternativ sollte eine unwiederbringliche Löschung der Daten vertraglich vereinbart sein.

Benutzen Sie für Papierunterlagen mit personenbezogenen Daten einem dafür vorgesehenen Datenschutzcontainer oder einen Aktenschredder!

DATENPANNEN, DATENKLAU ODER DATENVERLUST

Eine Datenpanne liegt vor (digital oder in Papierform) wenn es zur Vernichtung, zum Verlust, zur Veränderung, zur unbefugten Offenlegung von personenbezogenen Daten oder zum unbefugten Zugang zu personenbezogenen Daten kommt.

Beispiele dafür sind:

Versand eines Faxes oder einer E-Mail an den falschen Adressaten; versehentlicher Newsletterversand an E-Mail-Empfänger unter CC; Verlust eines USB-Sticks, Diensthandys oder -laptops mit personenbezogenen Daten; Diebstahl von Unterlagen bei einem Einbruch; ein Hackerangriff auf die Webseite oder das IT- System.

Dokumentieren Sie umgehend den Hergang und machen Sie eine Bestandsaufnahme.

Ein unterstützendes Formular zur Aufnahme einer Datenpanne finden sie zum Download unter:

https://datenschutz.ekd.de/infothek-items/arbeitshilfe-zur-meldung-von-datenpannen/

Setzen Sie sich in jedem Fall unverzüglich mit dem Verantwortlichen für den Datenschutz und ggfs. mit dem Datenschutzbeauftragten in Verbindung, da in bestimmten Fällen auch die Betroffenen selbst informiert werden müssen.

Führt ein solcher Datenschutzvorfall zu einem nicht unerheblichen Risiko für die Rechte einer betroffenen Person, meldet die verantwortliche Stelle dies unverzüglich der Aufsichtsbehörde, §32 DSG-EKD.

BEACHTEN SIE IN DIESEM FALL DIE HINWEISE AUF DER RÜCKSEITE DIESER FIBEL!

MESSENGERDIENSTE (Z.B. WHATSAPP)

Darf WhatsApp aufs Diensthandy?

Die Antwort lautet eindeutig **nein**!! Der Dienst ist weder besonders sicher, noch entspricht er den Anforderungen an den Datenschutz.

Auf Instant Messenger müssen Sie dennoch nicht verzichten:

Mit den Diensten Threema und Signal gibt es Alternativen. Alle Dienste sind sehr sicher und werden den Anforderungen des DSG-EKD gerecht.

Die Verbreitung von WhatsApp im privaten Umfeld ist sehr hoch, lassen Sie sich davon jedoch nicht entmutigen, die Installation eines alternativen Messenger vorzuschlagen oder durchzusetzen.

In kleineren Gruppen ist die gemeinsame App-Installation meist in wenigen Minuten erledigt.

II. DATENSCHUTZGRUNDSÄTZE

1. HISTORIE

Das Recht an den eigenen Daten wird aus dem Grundgesetz abgeleitet:

Es ist eine besondere Ausprägung des allgemeinen Persönlichkeitsrechts gem. Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG (Grundrecht auf freie Entfaltung der Persönlichkeit in Verbindung mit dem Grundrecht auf Menschenwürde).

Dieses „Recht auf informationelle Selbstbestimmung" wird als das Recht des Einzelnen verstanden, grundsätzlich selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu bestimmen.

Deswegen gilt: Die Verarbeitung personenbezogener Daten ist verboten, außer es gibt eine Rechtsgrundlage dafür.

2. DIE DSGVO UND DAS DSG-EKD

Seit dem 25.5.2018 gilt die Verordnung EU 2016/679 unter dem Titel „Datenschutz-Grundverordnung" (DSGVO). Diese Verordnung ist in allen europäischen Mitgliedsstaaten unmittelbar anwendbares Recht.

Art. 91 DSGVO gestattet den Kirchen, ihr bestehendes Datenschutzrecht fortzuführen, sofern dieses mit der DSGVO in Einklang steht. Dies führte zur Reform des EKD-Datenschutzgesetzes.

Am 24.5.2018 trat das Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland, DSG-EKD, in Kraft.

Gem. § 1 DSG-EKD ist der Schutzzweck des Kirchengesetzes, die einzelne Person davor zu schützen, dass sie durch den Umgang mit personenbezogenen Daten in ihrem Persönlichkeitsrecht beeinträchtigt wird.

IM ZENTRUM STEHT: DIE PERSONENBEZOGENEN DATEN

Personenbezogene Daten sind Angaben über eine bestimmte oder eine bestimmbare Person, d.h. alles, was geeignet ist, einen Menschen zu identifizieren, § 4 Nr. 1 DSG-EKD.

Dazu gehören natürlich der Name, die Adresse und Telefonnummern, Geburtsdatum, Mailadresse, Kontodaten, auch IP-Adresse; das können aber auch viele andere Informationen sein, durch die eine Person identifizierbar ist oder in Kombination identifizierbar wird.

Verarbeitung ist jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang, d.h. jede Art des Umgangs mit personenbezogenen Daten (z.B. das Erheben, Erfassen, Ordnen, Speichern, Übermitteln, Abgleichen u.a.m.), § 4 Nr. 3 DSG-EKD.

Die Verarbeitung auf Papier ist damit genauso gemeint wie die elektronische Verarbeitung. Ausnahme ist eine Verarbeitung ausschließlich für persönliche oder familiäre Zwecke, § 3 Abs. 4 DSG EKG.

GRUNDSÄTZLICH GILT:

Je sensibler die Daten sind (Gesundheitsdaten, Daten über religiöse oder weltanschauliche Überzeugungen, über die sexuelle Orientierung, die rassische oder ethnische Herkunft) desto besser müssen sie geschützt sein:

Im Zeitalter der digitalen Daten können z.B. Kriminelle mit den richtigen Daten erheblichen Schaden anrichten: Betrug, Erpressung, Identitätsdiebsstahl oder -missbrauch.

3. VERANTWORTUNG FÜR DEN DATENSCHUTZ

Der/die Verantwortliche einer Organisation ist auch der/die Verantwortliche für den Datenschutz und muss für die Einhaltung der Datenschutzvorschriften durch alle Mitarbeiter und Mitarbeitenden sorgen, z.B. durch eine entsprechende Verpflichtung und Schulung der Mitarbeiter.

Außerdem ist der/die Verantwortliche rechenschaftspflichtig für die Einhaltung der Grundsätze der Datenverarbeitung und der Dokumentationspflichten.

4. EINHALTUNG DATENSCHUTZRECHTLICHER PRINZIPIEN

Die Verarbeitung personenbezogener Daten orientiert sich u.a. an folgenden Grundsätzen (§ 5 DSG-EKD)

- **Rechtmäßigkeit**: Verarbeitung nach Treu und Glauben, Transparenz: Die Verarbeitung hat auf eine für die betroffene Person nachvollziehbare Weise zu erfolgen.

- **Zweckbindung**: Die Verarbeitung erfolgt für festgelegte, eindeutige und legitime Zwecke.

- **Datenminimierung**: Die Verarbeitung wird auf das dem Zweck angemessene und notwendige Maß beschränkt.

- **Integrität und Vertraulichkeit:**
  Die Daten sind vor Verlust, vor dem unberechtigten Zugriff Dritter und vor eventueller Veränderung zu schützen.

5. RECHTMÄSSIGKEIT DER DATENERHEBUNG

Bei der Verarbeitung personenbezogener Daten gilt, dass diese verboten ist, außer sie ist erlaubt, wie z.B. in folgenden Fällen (§ 6 DSG-EKD):

- Die Verarbeitung beruht auf einer Rechtsvorschrift (Nr. 1).
- Die Verarbeitung ist zur Erfüllung der Aufgaben der kirchlichen Stelle erforderlich (Nr. 3) oder zur Wahrnehmung einer sonstigen Aufgabe, die im kirchlichen Interesse liegt (Nr. 4).
- Die Verarbeitung ist für die Erfüllung eines Vertrags oder einer Vertragsanbahnung notwendig (Nr. 5).
- Die betroffene Person hat ihre Einwilligung zur Verarbeitung zu einem bestimmten Zweck gegeben (Nr. 2). Für die Rechtmäßigkeit der Einwilligung muss die betroffene Person über die Möglichkeit des Widerrufs für die Zukunft informiert worden sein (§ 11 Abs. 3 DSG-EKD).

6. BEACHTUNG DER BETROFFENENRECHTE, §19-25 DSG-EKD

Kommen Auskunftsanfragen von Betroffenen oder z.B. Anfragen auf Berichtigung, Löschung oder Einschränkung der Verarbeitung, dann ist es wichtig, dass diese in Absprache mit dem Verantwortlichen und dem Datenschutzbeauftragten unmittelbar bearbeitet werden.

NOTIZEN

NOTIZEN

Für weitere Informationen zum Datenschutz sprechen Sie bitte Ihren örtlich Beauftragten für den Datenschutz an!

Pommerscher Evangelischer Kirchenkreis

datenschutz@pek-nk.de

+49 (0) 151-11074156

Datenschutzaufsicht

Der Beauftragte für den Datenschutz der EKD

Lange Laube 20, 30159 Hannover

Telefon: +49 (0)511 768128-0

E-Mail: info@datenschutz.ekd.de

Web: https://datenschutz.ekd.de

LAYOUT
OVORO | ONLINE VOR ORT :: MAIL: KONTAKT@OVORO.DE

Bilder
Illustrationen: Hannah Jakobi
Cover - Pixabay: © TheDigitalArtist
Impressum - Pixabay: © Gerd Altmann
S. 18 - © rawpixel.com

HERAUSGEBER

dsgvoNORD GmbH
Marga-Faulstich-Str. 8 - 24145 Kiel
Telefon: 0431 301 400 600
Telefax: 0431 301 400 609
E-Mail: info@dsgvo-nord.de
Web: www.dsgvo-nord.de
REDAKTION Bettina Schneider
Manuel Langeheinecke

Pommerscher
Evangelischer Kirchenkreis

VERHALTEN BEI IT-NOTFÄLLEN

Ruhe bewahren & IT-Notfall melden

Lieber einmal mehr als einmal zu wenig anrufen!

Im Notfall wenden Sie sich an:

Team IT und Digitalisierung	0151-53910835
IT-Sicherheitsbeauftragte	0151-11074156

- Wer meldet?
- Welcher Arbeitsplatz ist betroffen?
- Wie bzw. mit welchen Programmen haben Sie gearbeitet?Was haben Sie beobachtet?
- Wann ist das Ereignis eingetreten?
- Wo befindet sich der betroffene Arbeitsplatz? (Gebäude, Raum)

Verhaltenshinweise

Weitere Arbeiten am IT-System **SOFORT** einstellen | Beobachtungen dokumentieren | Maßnahmen nur nach Anweisung einleiten

Herausgeber: Bundesamt für Sicherheit in der Informationstechnik
https://www.allianz-fuer-cybersicherheit.de/ACS/IT-Notfallkarte