WAS SIE JETZT BEACHTEN MÜSSEN – 800 JAHRE KIRCHLICHER DATENSCHUTZ

Vor etwa 500 Jahren hat ein Abt in Würzburg, Johannes Trithemius (1462 – 1516), als Erster die noch heute gültigen Grundlagen der Verschlüsselung beschrieben. Das spornt an, gerade in der Kirche diese Tradition zu wahren.

Wenn wir heute von Verschlüsselung sprechen, denken wir meist an Geheimdienste. Als Köpfe vermuten wir geniale Wissenschaftler, Mathematiker in Bletchley Park oder dem Pentagon. So ist es aber nicht. Der Abt Johannes, der nie eine Universität besuchte, hat seine Ideen dazu in der Abgeschiedenheit eines bayerischen Klosters entwickelt und wurde u. a. dadurch zu einem der größten Pioniere seiner Zeit.

Beachten Sie, dass das Post- und Fernmeldegeheimnis in aller Regel bei IT-Systemen nicht gilt. Deshalb ist Sicherheit gerade bei E-Mails so wichtig. Mit der „3-Z-Regel“ (siehe Innenseiten) leben Sie kirchliche Tradition und helfen, Daten verantwortungsvoll zu schützen. Passwörter spielen da eine wichtige Rolle. Ein im Jahr 1508 verfasstes Werk von Johannes war übrigens auch mit einem Passwort geschützt. Nach fast 500 Jahren hat man es 1998 entschlüsselt. So stellt man sich ein sicheres Passwort vor!

Weitere Informationen und alle Flyer zum Download finden Sie auf der Website des Bistums Regensburg unter:
www.bistum-regensburg.de ⇨ Einrichtungen A-Z ⇨ Datenschutz

Sie haben weitere Fragen?

Ihr zuständiger Datenschutzbeauftragter hilft Ihnen gerne bei Fragen oder Beschwerden weiter. Er unterstützt Sie auch, die relevanten Dokumente zu finden und nennt Ihnen bei Bedarf weitere Ansprechpartner. Bei ihm können Sie auch weitere Exemplare der Flyer bestellen.

Dr. Marcus Willamowski
Betrieblicher Datenschutzbeauftragter
für das bischöfliche Ordinariat
Telefon: 0941 597-1024
E-Mail: datenschutz.bo@bistum-regensburg.de

Gerhard Bielmeier
Betrieblicher Datenschutzbeauftragter
der Dekanate und Kirchenstiftungen
Telefon: 0941 597-1028
E-Mail: datenschutz.pfarreien@bistum-regensburg.de

Als betroffene Person oder betroffene Stelle haben Sie auch die Möglichkeit, sich direkt mit einer Beschwerde an die Datenschutzaufsicht zu wenden:

Jupp Joachimski
Datenschutzbeauftragter für die bayerischen (Erz-)Diözesen
Kapellenstr. 4
80333 München
Telefon: 089 2137-1796
E-Mail: JJoachimski@eomuc.de

Bischöfliches Ordinariat Regensburg
HA Zentrale Aufgaben / Generalvikariat
Fachstelle Datenschutz
Niedermünstergasse 1, 93047 Regensburg

Impressum

Herausgeber	Bischöfliches Ordinariat
Kontakt	Niedermünstergasse 1, 93047 Regensburg
Gestaltung	creativconcept werbeagentur GmbH

BISTUM REGENSBURG

Gib Acht

KIRCHLICHER DATENSCHUTZ – LEICHT GEMACHT!

1 DATENSCHUTZ BEGINNT AM ARBEITSPLATZ

Stand: November 2018

8 TIPPS FÜR ERFOLGREICHEN DATENSCHUTZ

1

Datenschutz beginnt mit dem Passwort

Wichtig ist, dass Sie für Ihren Rechner ein Passwort wählen, das schwer zu knacken ist. Ebenso wichtig ist es, dieses regelmäßig zu ändern. Es geht nämlich nicht nur darum, zu verhindern, dass jemand an Ihr Passwort gelangt – derjenige wird darauf achten, dass Sie gar nichts davon merken. Sollte das also der Fall sein, schneiden Sie mit dem Wechsel des Passworts auch bereits erfolgten Attacken die Lebensader ab.

2

Befolgen Sie die Passwort-Richtlinie

Computer arbeiten mit Millionen Rechenleistungen pro Sekunde extrem schnell. Oft dauert es nur ein paar Minuten, bis ein unsicheres Passwort geknackt ist. **Spezialisten haben deshalb eine Passwort-Richtlinie festgelegt, an deren Anforderungen Sie sich u. U. bei der Wahl Ihres Passworts halten müssen.** Falls dieses dennoch geknackt werden sollte, haben Sie wenigstens Ihren Beitrag geleistet.

3

Lassen Sie keine sensiblen Daten auf Ihrem Schreibtisch liegen

Ein Zettel mit der Handynummer Ihres Chefs am Bildschirm, die Personalakte oder sogar die Notiz mit dem Passwort neben der Tastatur? Jeder, der an Ihrem Schreibtisch vorbeigeht, kann diese Daten einsehen, obwohl sie nicht für fremde Augen bestimmt sind. **Achten Sie immer darauf, dass der Zutritt zu Ihrem Arbeitsplatz, der Zugang zu Ihrem Computer und der Zugriff auf Ihre Daten gut geschützt sind (3-Z-Regel).**

4

Geben Sie Ihre Zugangsdaten nicht weiter

Hilfsbereitschaft unter Kollegen ist Gold wert, das steht fest. Auf dem Nachhauseweg dem Kollegen im Büro nochmal das Passwort zuzurufen, damit er noch für morgen früh den Anhang einer Mail ausdruckt, klingt vielleicht nach einem Freundschaftsdienst, entpuppt sich jedoch als Bärendienst. **Behalten Sie Ihre Zugangsdaten deshalb unbedingt für sich und geben Sie diese niemals an Dritte weiter.**

5

Schützen Sie vertrauliche E-Mails vor dem Versenden

Früher hat man Briefe versiegelt. Heute werden Sie zumindest noch zugeklebt. Aber wie sieht es mit E-Mails aus? Gehen Sie hier auch auf Nummer sicher? **Wenn Sie vertrauliche Daten elektronisch versenden, sollten Sie den Anhang mit einem Passwort versehen.** Denken Sie bitte auch daran, das Passwort gesondert zu senden.

6

Sperren Sie beim Verlassen des Arbeitsplatzes Ihren Computer

Nur mal kurz einen Kaffee holen? Das Büro deswegen abzusperren lohnt sich wahrscheinlich nicht. **Ihren PC sollten Sie beim Verlassen des Arbeitsplatzes sperren. Das geht ganz einfach mit der Tastenkombination Windows + L.** Mit etwas Übung wird dieser Handgriff für Sie schnell zur Routine.

7

Sperren Sie am Feierabend oder bei längeren Pausen Ihr Büro ab

Ihr Computer schaltet sich ab, wenn er eine Weile nicht benutzt wird. Ihr Büro schließt sich aber nicht von selbst ab, wenn Sie längere Zeit Ihren Platz verlassen oder abends nach Hause gehen. Dann könnte man ungestört in Ihren Daten wühlen. **Schieben Sie Eingriffen einen buchstäblichen Riegel vor, indem Sie Ihr Büro immer gewissenhaft abschließen.** Sollte dies nicht möglich sein, sperren Sie zumindest Schubladen und Schränke mit sensiblen Daten ab.

8

Richten Sie einen Bildschirmschoner ein

Vergesslichkeit ist menschlich. **Haben Sie vergessen den Rechner vor dem Verlassen des Arbeitsplatzes zu sperren, erweist Ihnen ein automatischer Bildschirmschoner gute Dienste.** Dieser springt an, wenn der Computer fünf Minuten nicht verwendet wurde und kann nur durch die Eingabe Ihres Passworts beendet werden. Die Einrichtung ist ganz einfach (Rechtsklick auf dem Desktop und dann unter dem Menüpunkt „Anpassen") – so ist auch das spontane Schwätzchen in der Kaffeeküche kein Problem mehr.

NÄCHSTER FLYER:

2 EINWILLIGUNG ZUR DATENVERARBEITUNG