WAS SIE JETZT BEACHTEN MÜSSEN – 800 JAHRE KIRCHLICHER DATENSCHUTZ

Die Bank des Vertrauens oder der vielfach genutzte und positiv bewertete Online-Shop mit dem leicht zu erkennenden Logo schickt Ihnen eine wichtige Nachricht, die eine umgehende Reaktion erforderlich macht. Dafür wird schnell, kostenlos und unbürokratisch ein Antwortlink bereitgestellt, über den Sie alle Informationen mitteilen können. Hand aufs Herz, wer denkt dabei als Erstes an Betrug?

Sie sind lästig, aufdringlich und manchmal sogar ziemlich gut getarnt: Phishing Mails (Phishing = Kunstwort aus Passwort und Fishing) landen bei vielen von uns regelmäßig im Postfach. Sie versuchen uns zu täuschen, falsches Vertrauen zu erwecken und dadurch an unsere Zugangs- oder Bankdaten zu gelangen. Aber auch im persönlichen Kontakt, z. B. am Telefon, werden wir häufig um Auskünfte gebeten, die nicht für fremde Ohren bestimmt sind. Ohne Nachweis können wir nicht einmal sicher sein, ob es sich dabei tatsächlich um die Person handelt, die sie vorgibt zu sein.

Wichtig ist also, dass wir im Umgang mit persönlichen Daten besonders vorsichtig vorgehen und unser Gegenüber stets identifizieren, bevor wir überhaupt erst in Erwägung ziehen, sensible Informationen preiszugeben.

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!

4 GEBEN SIE DATEN NICHT AN FREMDE WEITER

Stand: Mai 2019

8 TIPPS FÜR ERFOLGREICHEN DATENSCHUTZ

1

Erteilen Sie Unbekannten keine Auskünfte

Das Ausspähen von Daten ist so prominent, dass es sogar Begriffe dafür gibt. Vielleicht haben Sie schon von Phishing oder Social Engineering gehört. Datendiebe nutzen jede Möglichkeit, an Daten zu kommen. Oft sind es unwissende Mitarbeiter, die sich mit mehr oder weniger Anstrengung überzeugen lassen, Daten preiszugeben. **Wenn Sie jemanden nicht kennen, dann geben Sie ihm auch keine Informationen weiter. Eigentlich ganz einfach.**

2

Identifizieren Sie Ihr Gegenüber, bevor Sie Daten preisgeben

Gefährlich wird es, wenn sich Dritte plausibel für einen Berechtigten ausgeben. Bestehen Sie im Zweifel auf eine zusätzliche Identifikation. Aber auch, wenn die Identität der Person nachgewiesen werden konnte, und es sich tatsächlich z. B. um einen neuen Mitarbeiter, den Mitarbeiter einer externen Firma für den Support oder den Ehepartner des Abteilungsleiters handelt, muss anschließend noch geprüft werden, ob der- oder diejenige überhaupt dazu berechtigt ist, die Daten zu erhalten.

3

Notieren Sie sich, wie sich ein Anrufer ausgewiesen hat

Ein Anrufer wird den Ausweis nicht durch das Telefon reichen können. Nutzen Sie wie viele professionelle Organisationen die Möglichkeit einer anderweitigen Identifizierung. Oft reicht die Frage nach dem Geburtsdatum oder dem Mädchennamen der Mutter, um Gut oder Böse zu erkennen. **Geben Sie im Zweifel keine Auskunft und bieten Sie stattdessen einen Rückruf unter einer Ihnen bekannten Telefonnummer an.**

4

Informieren Sie Ihren Vorgesetzen, wenn Sie zur Datenpreisgabe gedrängt werden

Versuche des Datenklaus über Phishing sind meist systematisch angelegt, um die „Schwachstelle Mensch“ auszunutzen. Leichtgläubigkeit, Neugierde und Hilfsbereitschaft sind neben Angst vor negativen Konsequenzen geeignete Ansatzpunkte zur Manipulation der Mitarbeiter. **Werden Sie Opfer eines solchen Betrugs, sollten Sie sich sofort an Ihren Vorgesetzten wenden, damit dieser entsprechend handeln und die Kollegen vorwarnen kann.** Das entlastet dann wiederum auch Sie.

5

Nehmen Sie Anfragen schriftlich auf

Betroffene haben umfassende Rechte. Sie aber auch. Nicht jedes Anliegen ist sofort und bedingungslos zu erfüllen. **Notieren Sie sich das Anliegen des Betroffenen (z. B. Anfragen nach Auskunft, Löschung etc.), denken Sie darüber nach und besprechen Sie es mit Ihren Kollegen, Vorgesetzten oder dem Datenschutzbeauftragten.** Möglicherweise ist die Rechtsausübung des Betroffenen gegen andere Gesetze, Vorschriften oder Interessen abzuwägen und dem Anliegen ist nicht, nicht sofort oder nicht in vollem Umfang zu entsprechen.

6

Verpflichten Sie Ihre Mitarbeiter und Dienstleister auf das Datengeheimnis

Vertraulich zu arbeiten, weil sich das so gehört, ist eine gute Sache. Für bestimmte Arten der Datenerfassung erfordert das Gesetz aber eine besondere schriftliche Vertraulichkeitsvereinbarung. **Damit dies in der Gemengelage des Alltags nicht untergeht, ist es sinnvoll, die Mitarbeiter von Anfang an schriftlich auf die Vertraulichkeit – und in unserem Fall auf das Datengeheimnis nach dem kirchlichen Datenschutz – zu verpflichten.**

7

Beantworten Sie keine E-Mails, die nach Ihren Zugangsdaten fragen

Geben Sie niemals Ihre Zugangsdaten preis, wenn Sie per Mail dazu aufgefordert werden. Datenschützern zufolge sind ausnahmslos alle derartigen E-Mails Fallen, die darauf abzielen, an Ihre Daten zu gelangen. Das gilt z. B. für das Versprechen, Ihnen ein 15-Millionen-Dollar-Vermögen aus einer nigerianischen Bank zukommen zu lassen, genauso wie für den vermeintlichen Kontoauszug von PayPal oder die Verpflichtung zur Annahme einer Datenschutzerklärung.

8

Melden Sie einen Fehler unverzüglich

Jedem von uns kann mal ein Fehler unterlaufen. Das ist ganz natürlich. Fehler in dem sensiblen Bereich von Zugangsdaten und vertraulichen Informationen rächen sich erfahrungsgemäß sehr schnell und sehr stark. **Helfen Sie mit den Schaden zu begrenzen, indem Sie ein Versehen dieser Art sofort dem Datenschutzbeauftragten melden. Dieser hilft dabei, den Fehler wieder zu bereinigen.**

NÄCHSTER FLYER:

5 REGELMÄSSIGE DATEN-SICHERUNG UND -VERNICHTUNG