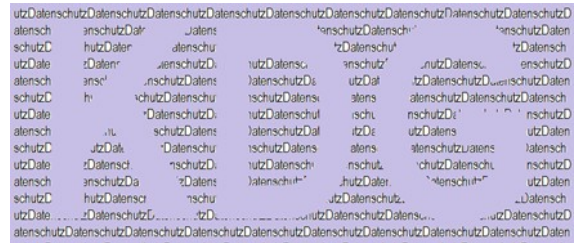


Betriebliche Datenschutzstelle
im Bistum Speyer



INFORMATIONEN ZUM DATENSCHUTZ

November 2023

Sehr geehrte Kolleginnen und Kollegen,

nachdem für viele von Ihnen die Datenschutzschulung schon länger zurück liegt, möchte ich Ihnen die wichtigsten Datenschutzmaßnahmen in Erinnerung rufen und Sie über aktuelle Bedrohungen informieren.

Leider mussten wir gerade erleben, dass auch wir nicht vor betrügerischen Angriffen ausgenommen sind. Es besteht täglich die Gefahr, dass Daten geklaut und anschließend für Straftaten verwendet werden. Nicht nur im dienstlichen Kontext sondern auch verstärkt im privaten Bereich. Gerade kürzlich habe ich



© Greser & Lenz, GDD Datenschutz-Cartoons

von einer Bekannten gehört, dass Sie auf eine Phishing-Mail hereingefallen ist und nun dadurch Probleme hat. Die Mail kam angeblich von DHL und besagte, dass zur Auslieferung der bestellten Ware noch eine Nachzahlung von 0,47 EUR erforderlich sei. Da sie das kürzlich bestellte Päckchen erhalten wollte und der Betrag ja gering ist, hat sie Ihre Daten eingegeben. Den Betrügern ging es dabei nicht um den geringen Betrag, sondern um die (Mastercard)Daten, die auch gleich für eine Bestellung verwendet wurden.

Auch die angeblich neue Errungenschaft für unser Privat- und Berufsleben - die Künstliche Intelligenz (KI) -, drängt in immer mehr Bereiche. Aber Vorsicht bleibt geboten, denn gerade (alte) Betrugsmaschinen, wie z. B. der Enkeltrick, kann dadurch noch „professioneller“ und zu einer erhöhten Gefahr werden. Aber auch durch KI unterstützte gesammelte Informationen, können falsche Aussagen enthalten.

Seien Sie daher auf der Hut und geben, trotz Hektik und Stress, (Ihre) Daten nicht zu schnell und unüberlegt an Dritte weiter.

Herzliche Grüße aus der Betrieblichen Datenschutzstelle

Ergänzende Informationen

<https://www.verbraucherzentrale.de/wissen/digitale-welt/datenschutz/welche-folgen-identitaetsdiebstahl-im-internet-haben-kann-17750>

<https://www.ndr.de/fernsehen/sendungen/markt/Dreister-Enkeltrick-mit-KI-Betrueger-nutzen-Audio-Deepfakes-/markt16728.html>

Von (Cyber) Angriffen bis (betrügerische) Zahlungen

Der Hackerangriff auf einem Server des Bischöflichen Ordinariats hat gezeigt, dass wir einer ständigen Gefahr ausgesetzt sind. Das Eindringen in Systeme kann dabei durch unterschiedliche Sicherheitslücken ermöglicht werden:

- 1) Technische Sicherheitslücken; an dieser Stelle sind wir davon abhängig, dass Sicherheitslücken von den Herstellern der Software rechtzeitig entdeckt und durch Sicherheits-Updates geschlossen werden können
 - 2) Menschliche Sicherheitslücken; **um diese Gefahr zu bannen benötigen wir dringend Ihre Mithilfe!**
- ⇒ Leider können unsere technischen Sicherheitsmaßnahmen nicht immer und alle gefährdeten E-Mails automatisch aussortieren, weshalb vereinzelt immer wieder welche in Ihrem Postfach landen. Meist sind diese mit einem LINK oder einem Anhang versehen, der Sie auf eine manipulierte Internetseite führt um persönliche Kontaktdaten oder Passwörter abzufragen (<https://www.verbraucherzentrale.de/wissen/digitale-welt/phishingradar/phishingmails-woran-sie-sie-erkennen-und-worauf-sie-achten-muessen-6073>) oder im Hintergrund eine Schadsoftware installiert (<https://www.verbraucherzentrale.de/wissen/digitale-welt/phishingradar/was-ist-ransomware-und-wie-kann-ich-mich-schuetzen-69789>).



Cyberangriff (Symbolbild) [CC BY-ND-NC 2.0](#) via flickr/[flowtastic](#)

- ⇒ Aber auch Mails ohne LINK oder Anhang, sondern nur mit einer Kontakt-Mail-Adresse können gefährlich sein. Denn die Sender wollen heraus finden, ob die Empfänger auf Anfragen reagieren. Sobald eine Reaktion erfolgt, startet der zweite Teil des Angriffs.
- ⇒ Natürlich beschränken sich solche Angriffe nicht auf den Mail-Verkehr, sondern erfolgen gleichfalls telefonisch, per SMS über Social Media Kanäle und auch schon als Termineinladung (<https://www.verbraucherzentrale.de/wissen/digitale-welt/phishingradar/gefahr-durch-falsche-termineinladungen-per-email-59701>).

Weitere Hinweise finden Sie auch direkt in der [Information zum Datenschutz 05 2012-12](#) auf unserer [Homepage](#) oder im Mitarbeiter PORTAL!

Grundregeln zum Datenschutz

Personenbezogene Daten dürfen grundsätzlich nur verarbeitet werden, wenn eine **Rechtsvorschrift** dies erlaubt oder eine wirksame **Einwilligung** des Betroffenen vorliegt. Dabei muss die Verarbeitung auf einen konkreten Zweck abgestellt sein. Eine Verarbeitung zu einem anderen Zweck ist nur unter strengen Vorgaben möglich. Bei der Verarbeitung (erfassen, speichern, ändern und löschen) ist auf eine **Datensparsame Nutzung** zu achten.

Bevor Sie Daten erheben, müssen Sie die Rechtmäßigkeit prüfen, sowie die Personen darüber informieren (**Informationspflicht = Datenschutzerklärung**), welche Daten Sie für welchen Zweck und vor allem auch wie lange verarbeiten.

Auch wenn alle Mitarbeiter:innen eine Verpflichtungserklärung zum Datenschutz unterzeichnet haben, ist dennoch darauf zu achten, dass nur berechtigte Personen Zugriff auf bestimmte Daten haben dürfen. Schützen Sie daher „Ihre“ Daten durch die vorgegebenen Maßnahmen (siehe auch IT-Gesetz im Bistum Speyer OVB 08/2018). Verschießen Sie Ihr Büro beim Verlassen und aktivieren Sie die Bildschirmsperre. Veranlassen Sie auch eine Passwortänderung und die Anpassung von Zugriffsberechtigungen auf Ordnersysteme und Programme, bei einem Stellenwechsel!

In manchen Bereichen müssen Daten auch **an andere Stellen weitergegeben** werden. Prüfen Sie vorab warum diese Stelle diese Daten benötigt und evtl. auch welche Angaben genau. Natürlich muss auch die Übermittlung datenschutzkonform erfolgen. Hierfür kann unsere Diözesan Cloud Communicare zum Einsatz kommen. Gerne beraten wir Sie bei der Prüfung sowie Umsetzung.

Leider sind nicht alle Systeme, Kommunikationsangebote und Softwarelösungen datenschutzkonform einsetzbar. Um hier die rechtlichen aber auch die sicherheitstechnischen Vorgaben ein zu halten, bedarf es immer vor dem **Einsatz neuer Systeme** einer internen Prüfung durch die Bereiche Rechtsamt, Datenschutz und EDV. Prüfungen werden durch die Kanzlei beauftragt und auch freigegeben.

Immer wieder kommt es vor, dass Personen von Ihrem **Auskunftsrecht** gebrauch machen. Dann wollen Sie wissen, welche Daten über Sie gespeichert werden und warum. Sollte eine solche Anfrage bei Ihnen auftauchen, dann setzen Sie sich umgehend mit der Datenschutzstelle in Verbindung, da es hierfür ein klar definiertes Verfahren gibt. Die Erfahrung zeigt, dass diese Personen oftmals nicht aus reinem Interesse handeln, sondern auf Grund einer Verärgerung oder eines anders gelagerten Vorfalles, weshalb diese Anfragen sehr sensibel und zeitnah bearbeitet werden müssen.

Oh, je eine **Datenpanne / Datenschutzverletzung**. Sollte Ihnen eine Datenpanne (z. B. ein Fehlversand an eine falsche Empfängeradresse) passiert sein, dann informieren Sie Ihren Vorgesetzten und setzen sich mit der Betrieblichen Datenschutzstelle in Verbindung, damit wir diese dokumentieren können, entsprechende Maßnahmen einleiten und ggfls. gemeinsam eine Meldung an die Aufsichtsbehörde durchführen zu können.

Wir ALLE tragen eine Mitverantwortung zum Schutz unserer Systeme und damit auch zum Schutz von Personendaten. Seien Sie wachsam und helfen Sie mit.

Sensibilisierung zum Umgang mit Social Media

Datenschutz bedeutet aus meiner Sicht auch der verantwortungsvolle Umgang mit sensiblen Informationen und persönlichen Darstellungen. Vielleicht nutzen Sie einen Messenger-Umstieg zur Sensibilisierung von Kindern und Jugendlichen, wie Sie sich und andere respektieren und vor allem schützen können.

Informationen und Materialien

<https://www.klicksafe.de/paedagogen-bereich/>

<https://youngdata.de/>

<https://www.handysektor.de/lernen>

<https://www.medien-kindersicher.de/startseite>

Noch Fragen . . .

- ⇒ Dann melden Sie sich gerne bei uns. Auch wenn wir gemeinsam mit Ihnen Beschwerden und Datenschutzverletzungen bearbeiten, so beraten wir Sie dennoch viel lieber im Vorfeld, um diese zu vermeiden: datenschutz@bistum-speyer.de
- ⇒ Schauen Sie doch mal wieder ins PORTAL für Mitarbeiter:innen. Die Darstellung hat sich verändert und evtl. müssen Sie einen Klick mehr machen. Aber es lohnt sich. Sie finden uns unter: [Arbeitsrechtliches und Co.](#) Dort finden Sie unter A-Z zum Datenschutz verschiedene Hinweise. Das Informationsblatt 12-2021 zu Spam- und Phishing-Mails, können Sie z. B. unter Formulare abrufen.
- ⇒ Wiederholen Sie doch einfach mal wieder die Online-Schulung zum Datenschutz. Unser Video-Konferenz System beinhaltet nicht nur ViKo-Räume, sondern auch Seminare wie z. B. die [Datenschutz Grundlagenschulung](#). Ein Hilfe-Formular finden Sie gleichfalls im PORTAL unter Schulungen.

Wunsch . . .

Ich würde mir wünschen, dass sich [das Image von Datenschutz als lästige Bürokratie] ändert:

Für die Sozialverbände in der Kirche, dass sie sich in die politische Debatte einbringen und den Wert von informationeller Selbstbestimmung stark machen, sich für den Schutz von Freiräumen und der Privat- und Intimsphäre und gegen Überwachung einsetzen.

Für die Jugendarbeit, dass dort Kinder und Jugendliche lernen, ihre eigenen Grenzen und Privatheitsbedürfnisse zu kennen und die anderer zu respektieren.

entnommen aus: <https://artikel91.eu/2021/03/23/drei-fragen-und-zwei-wuensche-zum-kirchlichen-datenschutz/#more-2269>

So erreichen Sie uns

Falls Sie Fragen haben oder Unterstützung benötigen, dann melden Sie sich:

**Betr. Datenschutzstelle
im Bistum Speyer**

06232 -102-240 oder

06232 -102-242

datenschutz@bistum-speyer.de

<https://www.bistum-speyer.de/bistum/aufbau/verwaltung/hazentralstelle/datenschutz/>