Bayerisches Landesamt für
Datenschutzaufsicht

Bayer. Landesamt für Datenschutzaufsicht | Postfach 1349 | 91504 Ansbach

Empfänger
Geschäftsführung
Straße
Plz Ort

Bayerisches Landesamt für Datenschutzaufsicht
Promenade 18 | 91522 Ansbach
Telefon: 0981 180093 0
Fax: 0981 180093 800
E-Mail: poststelle@lda.bayern.de
Web: www.lda.bayern.de

Ihre Kontaktperson

Online-Kennung zu Ihrer Prüfung **Aktenzeichen zu Ihrer Prüfung**

Ansbach,

Aufsicht nach Art. 58 Datenschutz-Grundverordnung (DS-GVO);
Präventionsprüfung zum Thema Absicherung von E-Mail-Accounts

Datenschutzrechtliche Prüfung Ihrer Organisation hinsichtlich technischer und organisatorischer Maßnahmen zum vorbeugenden Schutz gegen Cyberattacken auf E-Mail-Accounts (insb. Phishing)

Anlagen:
- **A** Prüfbogen „Absicherung von E-Mail-Accounts“
- **B** Anleitung zum Einreichen des digitalen Prüfbogens
- **C** Handreichung zum Prüfbogen
- **D** Informationsblatt „Absicherung von E-Mail-Accounts zum Schutz vor Phishing und Cyberattacken“

Sehr geehrte Damen und Herren,

das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) überwacht die Einhaltung des Datenschutzrechts im nicht-öffentlichen Bereich in Bayern, d. h. primär in den privaten bayerischen Wirtschaftsunternehmen, bei den freiberuflich Tätigen, in Vereinen sowie in Verbänden.

Seit mehreren Monaten können wir ein verstärktes Aufkommen von Cyberattacken auf E-Mail-Accounts von Verantwortlichen in Bayern registrieren. Oft steht das Abgreifen der enthaltenen vertraulichen E-Mail-Kommunikation im Vordergrund, um bspw. Finanztransaktionen zu manipulieren. Auch nachgelagerte Angriffe, die ein tieferes Eindringen in die Netzwerkstruktur ermöglichen oder die für die Weiterverbreitung von Schadsoftware auf die Systeme der Kontakte (z. B. Kunden) sorgen, finden statt. Bereits nach der Kompromittierung eines einzelnen E-Mail-Accounts werden von den Cyberkriminellen meist alle Kontakte mit gefälschten E-Mails angeschrieben.

Die eigentlichen Ursachen solcher Cyberangriffe sind nicht selten in einer unsachgemäßen Bedienung (u. a. auf Grund mangelndem Sicherheitsbewusstsein bei den Beschäftigten) oder in einer fehlerhaften Konfiguration und Absicherung der E-Mail-Accounts zu finden. Durch Homeoffice haben sich zudem in einigen Betrieben die diesbezüglich ohnehin schon bestehenden Sicherheitsgefährdungen weiter verschärft. Diesen kann jedoch aktiv mit

vertretbarem Aufwand entgegengewirkt werden, um die drohenden hohen Schäden – wirtschaftlich wie datenschutzrechtlich – für die eigene Organisation gering zu halten oder im Idealfall ganz zu vermeiden. Betrugsmaschen per E-Mail verursachten zuletzt für einzelne Betriebe Schäden im sechsstelligen Eurobereich und mehr.

Im Rahmen unserer gesetzlichen Aufgaben untersuchen wir mit den Fragen unserer beigefügten Präventionsprüfung zufällig ausgewählte Verantwortliche hinsichtlich grundlegender Sicherheitsanforderungen im Umgang mit E-Mail-Accounts nach Art. 32 DS-GVO. Ihr Prüfbogen liegt diesem Schreiben bei (Anlage A). Wir weisen darauf hin, dass Ihre Antwort ausschließlich über den digitalen Prüfbogen auf www.lda.bayern.de/kontrolle erfolgen sollte. Eine entsprechende Anleitung zur einfachen und sicheren Online-Einreichung ist diesem Schreiben beigefügt (Anlage B). Darüber hinaus informieren die Anlagen C und D zu wesentlichen Prüfpunkten und Hintergründen.

Wir fordern Sie auf, Ihre Antwort über unseren Online-Service auf www.lda.bayern.de/kontrolle unter Eingabe Ihrer individuellen Prüfkennung abzusenden. Eine Zusendung des beiliegenden Prüfbogens oder weiterer Unterlagen per Post, Fax oder E-Mail entfällt somit. Für den Eingang Ihrer (digitalen) Antwort haben wir uns spätestens den _____ vorgemerkt. Ihre Prüfkennung hierfür lautet:

Vorsorglich weisen wir Sie an dieser Stelle auf Folgendes hin: Sollten Sie dieser Aufforderung nicht fristgerecht nachkommen, stellen wir Ihnen den Erlass einer förmlichen Anweisung gem. Art. 58 Abs. 1 a) DS-GVO samt Zwangsgeldandrohung in Aussicht. Wir behalten es uns vor, im weiteren Prüfverlauf im Einzelfall auch vor Ort zu kontrollieren, um die Umsetzung der angegebenen Maßnahmen zu überprüfen. Ebenso können Dokumentationen und andere Unterlagen zu den abgefragten Themenschwerpunkten im weiteren Prüfverlauf angefordert werden.

Gesetzliche Informationen:

Die Datenschutz-Grundverordnung legt in Art. 58 Abs. 1 Buchstabe a fest, dass jede Aufsichtsbehörde über die Befugnis verfügt, den Verantwortlichen, den Auftragsverarbeiter und gegebenenfalls den Vertreter des Verantwortlichen oder des Auftragsverarbeiters anzuweisen, alle Informationen bereitzustellen, die für die Erfüllung ihrer Aufgaben erforderlich sind. Daneben verfügt jede Aufsichtsbehörde über die Befugnis, von dem Verantwortlichen und dem Auftragsverarbeiter Zugang zu allen personenbezogenen Daten und Informationen, die zur Erfüllung ihrer Aufgaben notwendig sind, zu erhalten (vgl. Art. 58 Abs. 1 Buchstabe e DS-GVO). Ein Verstoß gegen diese Verpflichtung stellt eine Ordnungswidrigkeit dar und kann mit einer Geldbuße geahndet werden.

Der Auskunftspflichtige kann die Auskunft auf solche Fragen verweigern, deren Beantwortung ihn selbst oder einen der in § 383 Abs. 1 Nrn. 1 bis 3 der Zivilprozessordnung bezeichneten Angehörigen der Gefahr strafgerichtlicher Verfolgung oder eines Verfahrens nach dem Gesetz über Ordnungswidrigkeiten aussetzen würde (§ 40 Abs. 4 Satz 2 Bundesdatenschutzgesetz). Die Inanspruchnahme des Auskunftsverweigerungsrechts ist mitzuteilen und nachvollziehbar zu begründen.

Mit freundlichen Grüßen

Dieses Schreiben wurde elektronisch erstellt und ist ohne Unterschrift gültig.

Hinweis zur Verarbeitung Ihrer personenbezogenen Daten

Verantwortlich für die Verarbeitung Ihrer personenbezogenen Daten im Rahmen des vorliegenden Kontakts ist das Bayerische Landesamt für Datenschutzaufsicht. Weitere Informationen zur Verarbeitung Ihrer Daten, insbesondere zu den Ihnen zustehenden Rechten, können Sie unserer Homepage unter www.lda.bayern.de/informationen entnehmen oder auf jedem anderen Wege unter den o. g. Kontaktdaten bei uns erfragen.