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

Telefon:
Fax:

Ihr Zeichen **Unser Aktenzeichen zu Ihrer Prüfung**

-

Ansbach, 30.11.2021

Aufsicht nach Art. 58 Datenschutz-Grundverordnung (DS-GVO);

Ransomware-Prävention – Datenschutzrechtliche Prüfung Ihrer Organisation hinsichtlich technischer und organisatorischer Maßnahmen zum vorbeugenden Schutz gegen Ransomware-Attacken

Anlagen:

- Prüfbogen (Ihr Antwortbogen)
- Handreichung zum Prüfbogen
- Informationsblatt zur Prüfung

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.

Zuletzt konnten wir auch in Bayern ein verstärktes Aufkommen sogenannter Ransomware-Attacken registrieren. Dabei handelt es sich um Sicherheitsvorfälle, bei denen Systeme der betroffenen Verantwortlichen angegriffen, die gespeicherten Daten verschlüsselt und die Opfer dadurch zu einer Lösegeldzahlung erpresst werden. Die Verfügbarkeit der für die tägliche Arbeit erforderlichen Systeme und Dienste ist in diesen Fällen gewöhnlich nicht mehr vollständig gegeben, sodass Produktionen und Abläufe nur noch eingeschränkt funktionieren oder still stehen. Nicht selten führen diese Art von Cyberattacken zu einem hohen Risiko für die Rechte und Freiheiten der betroffenen Personen, häufig zudem zu einem enormen wirtschaftlichen Schaden für die angegriffene Organisation.

Im Rahmen unserer gesetzlichen Aufgaben untersuchen wir mit den Fragen unserer beigefügten Ransomware-Präventionsprüfung zufällig ausgewählte Verantwortliche gezielt hinsichtlich grundlegender Sicherheitsanforde-

rungen, die bei Ransomware-Cyberattacken mitunter darüber entscheiden können, ob ein Angriff erfolgreich abgewehrt bzw. das Schadensausmaß aktiv begrenzt werden kann. Prüfgrundlage bilden somit die Schutzmaßnahmen zur Sicherheit der Verarbeitung nach Art. 32 DS-GVO.

Die schriftlichen Prüfunterlagen, die Ihnen nun vorliegen, bestehen aus einem Anschreiben, einem Prüfbogen, einer Handreichung zum Prüfbogen und einem Informationsblatt. Wir fordern Sie auf, im ersten Prüfschritt lediglich den beiliegenden **Prüfbogen** zu nutzen, um uns Ihre Stellungnahme zu den untersuchten Schwerpunkten zukommen zu lassen. Bestätigen Sie uns damit bei Ihnen durchgeführte Maßnahmen zur Sicherheit oder legen Sie bei Bedarf ergänzende Ausführungen zur Begründung bei, sollten manche Maßnahmen bei Ihnen bislang nicht ergriffen worden sein. Die Handreichung zum Prüfbogen stellt ausgewählte Maßnahmen in einer Art Checkliste als Hilfestellung für Sie dar. Im beilegenden Informationsblatt können Sie zudem allgemeine Hintergründe zur Prüfung und zum Schwerpunkt Ransomware erfahren.

Für den Eingang Ihres Prüfbogens haben wir uns spätestens den 22.12.2021 vorgemerkt.

Im weiteren Prüfverlauf behalten wir es uns vor, 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.