

Öffentliche Benachrichtigung nach § 34 KDG

Sehr geehrte Damen und Herren,

dies ist eine öffentliche Benachrichtigung wegen eines datenschutzrechtlich relevanten Vorfalls. Falls Sie mit uns bis Mai 2024 in Kontakt standen, können wir nicht ausschließen, dass theoretisch auch Ihre Daten aus mit uns erfolgter E-Mail-Korrespondenz davon betroffen sind. Ein Risiko bestand lediglich für einen sehr kurzen Zeitraum 31.05.2024 vom 1:00 Uhr in der Nacht bis 7:00 Uhr am Morgen. Seit 31.05.2024 nach 7:00 Uhr am Morgen sind unsere Systeme alle wieder gesichert.

Wir möchten Ihnen im Folgenden erklären, worum es geht und was dies für Sie theoretisch bedeuten kann.

Diese öffentliche Benachrichtigung nach § 34 KDG (Gesetz über den Kirchlichen Datenschutz) richtet sich an alle, deren personenbezogene Daten wir in unseren IT-Systemen auf Ebene der allgemeinen Verwaltung verarbeiten.

Am 31.05.2024 haben Angreifer über unser E-Mailsystem englischsprachige Spammails versendet. Inhalt dieser Spam-Mail war ein Link zu einem 100\$ Gutschein für einen Anbieter, der mit Kryptowährung handelt. Bei einem Klick auf den Link wäre man nicht auf der Originalwebseite des Anbieters, sondern auf einer „Fake“-Seite gelandet. Ziel dieser Spam-Mail war es wohl, Zugangsdaten dieser Kryptoplattform abzugreifen. Die Angreifer haben hierzu scheinbar E-Mail-Adressen aus der ganzen Welt als Empfänger gewählt, die in einer Datenbank gesammelt worden sind.

Wir haben keinerlei Feststellungen darüber, dass bestimmte personenbezogene Daten aus unseren Systemen bzw. speziell Ihre personenbezogenen Daten, sofern wir diese in unserem System zum damaligen Zeitpunkt gespeichert hatten, konkret betroffen sind. Gleichwohl können wir nicht ausschließen, dass personenbezogene Daten im Zusammenhang mit der Sicherheitslücke von Dritten abgegriffen wurden.

Als Vorsichtsmaßnahme haben wir unverzüglich unsere Systeme und Netzwerkverbindungen geprüft und die Herstellervorgaben unserer Softwareanbieter umgesetzt. Wir haben alle empfohlenen Maßnahmen der Aufsichtsbehörden zur Beseitigung der Sicherheitslücke beachtet.

Wir haben unverzüglich nach Kenntnis der Sicherheitslücke eine Anfrage bei der für uns zuständigen Datenschutz-Aufsichtsbehörde, dem Katholischen Datenschutzzentrum in Frankfurt am Main, gestellt. Von dort aus wurden wir ergänzend beraten und dabei unterstützt, die IT-Sicherheit wiederherzustellen. Mit entsprechender Unterstützung haben wir den Vorfall zudem als Datenschutzverletzung i.S.d. § 33 KDG eingestuft und das Risiko für möglicherweise betroffene Personen als „nicht völlig unerheblich“ i.S.d. § 34 KDG bewertet. Daher stellen wir Ihnen diese Informationen zur Verfügung.

Wir nehmen den Vorfall sehr ernst und arbeiten daran, weiterhin die Folgen der Sicherheitslücke und mögliche Auswirkungen für die Zukunft zu analysieren. Unser Ziel ist es, jegliche Auswirkungen auf personenbezogene Daten in unseren Systemen zu begrenzen und auszuschließen. Für Sie besteht aktuell kein Handlungsbedarf. Wir haben alles veranlasst, was möglich ist, um Auswirkungen der Sicherheitslücke zu verhindern. Wir haben keinen Hinweis darauf, dass gezielt nach bestimmten (Ihren) Daten gesucht wurde.

Allgemein gilt dennoch:

Sollten Sie Anhaltspunkte für eine missbräuchliche Verwendung Ihrer personenbezogenen Daten haben, empfehlen wir Ihnen, eine Anzeige bei Ihrer örtlichen Polizeibehörde zu erstatten. Ein sogenannter Identitätsmissbrauch, wenn also Dritte vortäuschen, in Ihrem Namen aufzutreten, ist eine Straftat.

Generell sollten Sie sich der Gefahr bewusst sein, dass Kriminelle, die, auf welche Weise auch immer, in den Besitz Ihrer personenbezogenen Daten gekommen sind, diese verwenden könnten, um Sie zu manipulieren, beispielsweise um weitere Informationen über Sie oder Dritte zu bekommen oder Sie zu einer unberechtigten Geldüberweisung oder Ähnlichem zu veranlassen. Dies gilt insbesondere bei Benutzung des Internets. Eine Gefahr kann z. B. auch von Dateianhängen an E-Mails, die von nicht vertrauenswürdigen Absendern stammen, ausgehen.

Denkbare Risiken einer missbräuchlichen Verwendung personenbezogener Daten können gesellschaftliche und wirtschaftliche Nachteile bzw. Reputationsschäden sein.

Bitte achten Sie insbesondere bei der Nutzung digitaler Medien auf Anzeichen, die kriminelle Handlungen zu Ihren Lasten nahelegen.

Bei Rückfragen stehen wir Ihnen gerne unter den nachfolgenden Kontaktinformationen zur Verfügung:

Caritasverband Bruchsal e.V.
Friedhofstr. 11
76646 Bruchsal
E-Mail: info@caritas-bruchsal.de

Kontaktinformationen unseres externen Datenschutzbeauftragten:

Jörg M. Leuchtner (Rechtsanwalt)
Freiburger Datenschutzgesellschaft mbH
Luisenstr. 5, 79098 Freiburg
Tel.: + 49 (0) 761 - 21716550
E-Mail: info@freiburger-datenschutzgesellschaft.de

Über weitere Erkenntnisse in diesem Zusammenhang werden wir bei Bedarf an gleicher Stelle informieren.

Mit dieser öffentlichen Bekanntmachung nach § 34 KDG erfüllen wir unsere gesetzliche Verpflichtung, Sie insbesondere vor einem möglichen Datenmissbrauch zu warnen.

Mit freundlichen Grüßen

Vorstand:

Sabina Stemann-Fuchs (Vorsitzende), Andreas Häuslpeiz