

Die Sicherheit unserer Produkte und digitalen Lösungen hat für uns einen hohen Stellenwert. Sollten Sie eine potenzielle Schwachstelle, Sicherheitslücke oder einen Sicherheitsvorfall im Zusammenhang mit einem unserer Produkte feststellen, bitten wir Sie, uns dies über das entsprechende Online-Formular mitzuteilen.

Ihre Meldung hilft uns, mögliche Sicherheitsrisiken frühzeitig zu erkennen, zu untersuchen und geeignete Maßnahmen zum Schutz unserer Produkte, Kunden und Nutzer einzuleiten.

Bitte beschreiben Sie die Schwachstelle möglichst genau und geben Sie – soweit bekannt – das betroffene Produkt, die Produkt- bzw. Software-/Firmware-Version, mögliche Auswirkungen und Schritte zur Reproduktion an. Screenshots, Logdateien oder andere technische Nachweise können Sie der Meldung beifügen.

Bitte übermitteln Sie keine personenbezogenen oder vertraulichen Daten Dritter, soweit diese für die Untersuchung nicht erforderlich sind.

1. Coordinated Vulnerability Disclosure (CVD)

Wir behandeln Meldungen nach den Grundsätzen der Coordinated Vulnerability Disclosure (CVD). Eingehende Meldungen werden geprüft, hinsichtlich ihrer Sicherheitsauswirkungen bewertet und erforderliche Maßnahmen zur Behebung oder Reduzierung des Risikos eingeleitet.

Bitte veröffentlichen Sie Informationen über eine noch nicht behobene Schwachstelle nicht, bevor wir Gelegenheit hatten, diese zu untersuchen und geeignete Abhilfemaßnahmen bereitzustellen.

Bei Sicherheitsprüfungen bitten wir Sie, keine Daten oder Systeme zu verändern oder zu beschädigen, nicht auf Daten Dritter zuzugreifen und die Verfügbarkeit von Produkten, Systemen oder Diensten nicht zu beeinträchtigen.

2. Cyber Resilience Act (CRA)

Meldungen werden von uns auch daraufhin geprüft, ob sich daraus gesetzliche Handlungs- oder Meldepflichten nach der Verordnung (EU) 2024/2847 (Cyber Resilience Act – CRA) ergeben.

Soweit die gesetzlichen Voraussetzungen vorliegen, nehmen wir die erforderlichen Meldungen, insbesondere zu aktiv ausgenutzten Schwachstellen und schwerwiegenden Sicherheitsvorfällen, gegenüber den nach dem CRA zuständigen Stellen vor.

3. Datenschutzhinweise

Verantwortlicher für die Verarbeitung der im Rahmen der Schwachstellenmeldung erhobenen personenbezogenen Daten ist die

EXHAUSTO GmbH, Im Niedergarten 14, 55124 Mainz.

Unseren Datenschutzbeauftragten erreichen Sie unter datenschutz@exhausto.de

Wir verarbeiten die von Ihnen übermittelten Daten, insbesondere Ihre Kontaktdaten, Angaben zum betroffenen Produkt, Informationen zur Schwachstelle bzw. zum Sicherheitsvorfall sowie gegebenenfalls übermittelte Dateien und technische Informationen, um Ihre Meldung entgegenzunehmen, zu prüfen und zu dokumentieren, Sicherheitsrisiken zu untersuchen und zu

beheben, mit Ihnen bei Rückfragen zu kommunizieren und gegebenenfalls gesetzliche Meldepflichten zu erfüllen.

Soweit die Verarbeitung zur Erfüllung gesetzlicher Verpflichtungen erforderlich ist, erfolgt sie auf Grundlage von Art. 6 Abs. 1 lit. c DSGVO in Verbindung mit den einschlägigen gesetzlichen Vorschriften, insbesondere der Verordnung (EU) 2024/2847 (Cyber Resilience Act – CRA). Im Übrigen erfolgt die Verarbeitung auf Grundlage von Art. 6 Abs. 1 lit. f DSGVO. Unser berechtigtes Interesse besteht in der Erkennung, Untersuchung und Behebung von Schwachstellen und Sicherheitsvorfällen sowie in der Gewährleistung der Sicherheit unserer Produkte, Systeme, Kunden und Nutzer.

Ihre Daten werden innerhalb unseres Unternehmens nur den Stellen zugänglich gemacht, die mit der Bearbeitung der Meldung befasst sind. Soweit erforderlich, können Daten außerdem an eingesetzte Dienstleister, betroffene Hersteller oder Lieferanten sowie aufgrund gesetzlicher Verpflichtungen an zuständige Behörden und Stellen übermittelt werden. Eine Übermittlung in Drittländer erfolgt nur unter Beachtung der Voraussetzungen der Art. 44 ff. DSGVO.

Wir speichern Ihre personenbezogenen Daten nur so lange, wie dies für die Untersuchung, Bearbeitung und Dokumentation der Meldung sowie zur Erfüllung gesetzlicher Aufbewahrungs-, Nachweis- und Meldepflichten erforderlich ist.

Die Angabe Ihrer Kontaktdaten ist freiwillig. Ohne eine Kontaktmöglichkeit können wir jedoch keine Rückfragen stellen und Sie nicht über den Bearbeitungsstand informieren.

Sie haben nach Maßgabe der gesetzlichen Voraussetzungen das Recht auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung und Datenübertragbarkeit. Soweit die Verarbeitung auf Art. 6 Abs. 1 lit. f DSGVO beruht, haben Sie außerdem das Recht, Widerspruch nach Art. 21 DSGVO einzulegen. Darüber hinaus haben Sie das Recht, sich bei einer Datenschutzaufsichtsbehörde zu beschweren.

Weitere Informationen zur Verarbeitung personenbezogener Daten und zu Ihren Rechten finden Sie in der Datenschutzerklärung unserer Homepage.

Sie haben gemäß DSGVO als betroffene Person, deren Daten wir verarbeiten, folgende Rechte:

- Recht auf Auskunft (Art. 15)
- Recht auf Berichtigung (Art. 16)
- Recht auf Löschung („Vergessenwerden“) (Art. 17)
- Recht auf Einschränkung der Verarbeitung (Art. 18)
- Recht auf Übertragung Ihrer Daten (Art. 20)
- Beschwerderecht bei der Aufsichtsbehörde (Art. 77)

Die für uns zuständige Behörde ist:

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz

Hintere Bleiche 34
55116 Mainz

Telefon: +49 6131 208-2449
Telefax: +49 6131 208-2497
E-Mail: poststelle@datenschutz.rlp.de
Homepage: <https://www.datenschutz.rlp.de>