Allgemeine Informationen

Meldestellen und Datenschutzhinweise für den schnellen Zugriff bei IT-Sicherheitsvorfällen.“

- Unterstützung: Hilfe und Anlaufstellen im Notfall

Unterstützung: Hilfe und Anlaufstellen im Notfall

Hier finden Sie eine strukturierte Übersicht wichtiger Notfall- und Meldestellen für Cybersicherheitsvorfälle, Strafverfolgung sowie Datenschutzverstöße (mit Fokus auf Baden-Württemberg sowie bundesweite Anlaufstellen).

> **Wichtiger Hinweis:** Bewahren Sie Ruhe, sichern Sie nach Möglichkeit Beweise und stimmen Sie kritische Maßnahmen (z. B. Abschalten oder Löschen von Systemen) im Zweifel vorab mit den Fachstellen ab.

Wichtige Telefonnummern und Meldestellen

Bereich / Stelle	Telefon	E-Mail / Web	Leistungen & Hinweise
Cyber-Ersthilfe BW *(Cybersicherheitsagentur BW)*	**0711 137-99999**	`cybererstthilfe@cybersicherheit.bwl.de`	**24/7 (rund um die Uhr)**, kostenfrei. Erste Einordnung, Erstanalyse und Handlungsempfehlungen für Unternehmen, Kommunen, Einrichtungen und Bürger in Baden-Württemberg.
Polizei: ZAC beim LKA BW *(Zentrale Ansprechstelle Cybercrime)*	**0711 5401-2444**	—	**24/7 (rund um die Uhr)** für Unternehmen und Behörden bei Cybercrime. Unterstützung bei Anzeigeerstattung und Spurensicherung.
BSI Service-Center *(Bundesamt für Sicherheit in der Informationstechnik)*	**0800 274 1000** *(kostenfrei)*	`service-center@bsi.bund.de`	Bundesweite Unterstützung und Einordnung von IT-Sicherheitsvorfällen (Servicezeiten i. d. R. Mo–Do 8:00–17:00 Uhr, Fr 8:00–16:00 Uhr).

LfDI Baden-Württemberg *(Landesbeauftragter für den Datenschutz und die Informationsfreiheit)*	**0711 61 55 41 - 0**	`poststelle@lfdi.bwl.de`	Zuständige Datenschutzaufsichtsbehörde in Baden-Württemberg u. a. für Fragen zum Datenschutz und zur Meldung von Datenschutzverstößen (Datenpannen).

Datenschutz & Datenpannen (DSGVO)

Wenn bei einem Cyberangriff oder IT-Vorfall **personenbezogene Daten** (z. B. Kundendaten, Beschäftigtendaten, Kontaktlisten) verloren gehen, unbefugt offengelegt werden oder unbefugte Dritte Zugriff erhalten, greifen Pflichten nach der Datenschutz-Grundverordnung (DSGVO):

- **Datenschutzbeauftragte/n einbinden:** Ziehen Sie frühzeitig Ihre interne oder externe Datenschutzbeauftragte / Ihren Datenschutzbeauftragten hinzu, um Risiko, Betroffenheit und Meldepflichten rechtssicher zu bewerten.
- **Aufsichtsbehörde (LfDI BW) melden:** Liegt voraussichtlich ein Risiko für die Rechte und Freiheiten natürlicher Personen vor, muss die Datenschutzverletzung der zuständigen Aufsichtsbehörde gemeldet werden – nach Möglichkeit **innerhalb von 72 Stunden** nach Bekanntwerden.
- **Betroffene Personen informieren:** Besteht voraussichtlich ein **hohes Risiko** für die persönlichen Rechte und Freiheiten der betroffenen Personen, müssen diese ebenfalls unverzüglich benachrichtigt werden.
- **Vorfall intern dokumentieren:** Halten Sie alle Fakten zum Vorfall, dessen Auswirkungen und die ergriffenen Maßnahmen intern fest (auch wenn im Einzelfall keine behördliche Meldepflicht besteht).

Kurz-Checkliste für die ersten Minuten

1. **Beweise & Logs sichern:** Keine unüberlegten Lösch- oder Neustartaktionen durchführen, die digitale Spuren vernichten könnten.
2. **Systeme isolieren:** Betroffene Geräte/Netzwerksegmente gezielt trennen, um eine Ausbreitung zu bremsen.
3. **Zugänge absichern:** Kritische Konten (z. B. Admin, E-Mail, VPN, Cloud) über ein sauberes Gerät prüfen und Zugangsdaten/Sessions absichern.
4. **Stellen informieren:** Cyber-Ersthilfe BW, Polizei (ZAC) sowie bei Bezug zu personenbezogenen Daten den Datenschutz und die LfDI BW einbinden.