



Incident Notification Policy

VERSION 1.0 · EFFECTIVE FROM 1 SEPTEMBER 2026 · LAST REVIEWED 22 JULY 2026

This policy explains how and when we notify our customers and the authorities about service outages, security incidents and personal data breaches.

1. Scope. This policy covers unplanned service outages, security incidents, and personal data breaches affecting the CashXChain platform.

2. Personal data breaches. Where we act as controller and a breach is likely to result in a risk to individuals, we notify the competent supervisory authority (the [Bayerisches Landesamt für Datenschutzaufsicht](#) ⁷) without undue delay and, where feasible, within 72 hours of becoming aware of it, in line with Article 33 [GDPR](#) ⁷. Where a breach is likely to result in a high risk to individuals, we notify the affected individuals without undue delay, in line with Article 34 GDPR. Where we act as processor for a business customer, we notify that customer without undue delay so it can meet its own obligations.

3. Service outages. We inform affected customers of significant unplanned outages, with the impact and the expected time to resolution, and we confirm when service is restored.

4. Security incidents. We investigate, contain and remediate security incidents, and we notify affected customers and authorities where the law or a contract requires it.

5. What our notifications contain. Where applicable, a notification describes the nature of the incident, its likely consequences, the measures taken or proposed, and a contact point for more information.

6. How we notify. We notify the account contact by email and, for wide-reaching incidents, publish updates on our status page.

7. Contact. Report a suspected incident to security@cashxchain.com; data-protection questions can be sent to privacy@cashxchain.com.