

Incident Response and Breach Notification Policy

Seba Agency UG (haftungsbeschränkt) · Version 1.0 · Effective **Oct 13, 2026** · Owner: Joshua Omosebi, Managing Director · Review: annually

1. Purpose and scope

This policy describes how Seba Agency detects, handles and reports security incidents and personal data breaches, including incidents affecting the TikTok Shop integration and data we receive from TikTok or from the seller we work for.

2. Definitions

- **Security incident:** any event that threatens the confidentiality, integrity or availability of our systems or data, for example a lost laptop, a phishing compromise, a leaked API token, unauthorised access to n8n or Notion, malware, or a server compromise.
- **Personal data breach:** a security incident leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data (Art. 4(12) GDPR).

3. Roles

- **Incident lead:** Joshua Omosebi, Managing Director, +49 176 70574768.
- **Deputy:** Joshua Omosebi, +49 176 70574768.
- **Everyone:** reports any suspected incident to the incident lead immediately by phone or message, and does not investigate alone or delete evidence.

4. Response steps

1. **Report and log:** record the time, what was observed and who reported it in the incident log (section 8).
2. **Contain:** for example revoke and rotate affected tokens and passwords, disable affected accounts, pause affected n8n workflows, block IP addresses, isolate the server.

3. **Assess:** what happened, which systems and data were affected, whether personal data is involved, how many people, and the likely risk to them.
4. **Notify:** see section 5.
5. **Recover:** restore from clean backups, fix the cause, re-enable services.
6. **Review:** within two weeks, record the root cause and preventive actions, and update policies where needed.

5. Notification

Data we process for a client (e.g. the TikTok Shop seller) and data received from TikTok

We notify the affected seller and TikTok **without undue delay, and no later than 48 hours** after becoming aware of a personal data breach, or within any shorter period required by contract or by TikTok's terms, so the controller can meet its own 72-hour deadline. As far as known at the time, the notice includes: the nature of the breach; categories and approximate number of people and records affected; likely consequences; measures taken or proposed; and a contact person (Art. 33(3) GDPR). Further information follows as soon as it is available.

Data for which Seba Agency is the controller

- We notify the competent supervisory authority, the Bayerisches Landesamt für Datenschutzaufsicht (BayLDA), within 72 hours, unless the breach is unlikely to result in a risk to individuals (Art. 33 GDPR).
- We inform affected individuals without undue delay if the breach is likely to result in a high risk to them (Art. 34 GDPR).

Every breach is documented in the incident log, including breaches that did not need to be reported (Art. 33(5) GDPR).

6. Quick playbooks

- **Leaked or exposed token or password:** revoke it immediately, issue a new one, check logs for misuse since exposure, and notify under section 5 if data was accessed.
- **Lost or stolen device:** lock or wipe it remotely if possible, sign out all sessions, rotate passwords of accounts used on it. With full-disk encryption this is usually not a breach, but it is logged.

- **Suspected server compromise:** take a snapshot for analysis, restrict the firewall to the admin's IP address, rotate every credential stored on the server, and rebuild from a clean image if the compromise is confirmed.
- **Phishing:** reset the password, revoke sessions, check 2FA settings and email forwarding rules.

7. Contacts

Who	Contact
Incident lead	Joshua Omosebi, joshua@sebaagency.com, +49 176 70574768
Deputy	Joshua Omosebi, joshua@sebaagency.com, +49 176 70574768
Seller (client)	Joshua Omosebi, joshua@sebaagency.com, +49 176 70574768
TikTok	Joshua Omosebi, joshua@sebaagency.com, +49 176 70574768
Supervisory authority	BayLDA, breach report form at lda.bayern.de
Hosting	Hetzner Online GmbH support

8. Incident log

Date	Description	Personal data involved?	Actions taken	Notified (who, when)	Closed

9. Testing and review

This policy is reviewed annually. Once a year we walk through one scenario from section 6 to check that contacts, access and steps still work.