

Data Classification and Handling 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 defines how Seba Agency classifies data and how each class must be stored, shared, encrypted, retained and deleted. It applies to all data we create, receive or process, in every system.

2. Classification levels

Level	Description	Examples
Public	Approved for publication	Website content, published case studies
Internal	Business information not meant for the public; low harm if disclosed	Internal processes, templates, meeting notes
Confidential	Personal data and client business data; disclosure could harm people or clients	Creator usernames and IDs, order IDs, SKU quantities, commission amounts, client ad performance, contact details
Restricted	Disclosure would give access to systems or cause serious harm	Passwords, API keys and tokens, the n8n encryption key, SSH keys, bank or payment data

When in doubt, the higher level applies.

3. Data processed by the TikTok Shop integration

Data	Level	Purpose
Creator usernames and creator IDs	Confidential	Attribute orders to creators

Data	Level	Purpose
Order IDs	Confidential	Match orders and commissions
SKU quantities	Confidential	Calculate commissions and performance
Commission amounts	Confidential	Commission tracking and payout reconciliation
TikTok API credentials	Restricted	Connect to TikTok APIs

Data minimisation: the integration does not request or store buyer names, delivery addresses, phone numbers or email addresses. If such data is ever received by mistake, it is deleted without delay and the workflow is corrected.

4. Handling rules

Rule	Internal	Confidential	Restricted
Where it may be stored	Company systems	Approved systems only (n8n, the Notion creator database)	Password manager, n8n credential store, Coolify environment settings only
Sharing	Team and approved contractors	Only people in the access register with a need to know; clients and partners only for the agreed purpose	Never in plain text; never in chat, email, Notion or documents
Export and download	Allowed	Only when needed; exported files deleted after use	Not allowed
Personal devices or private accounts	Avoid	Not allowed	Not allowed

5. Encryption

- **In transit:** all data is transferred over HTTPS with TLS 1.2 or higher, including TikTok APIs, n8n webhooks and editor, Notion and Tally.
- **At rest:**
 - Company devices use full-disk encryption (FileVault or BitLocker).
 - n8n stores credentials encrypted with its encryption key.
 - Notion encrypts data at rest according to its security documentation.
 - Backups are stored encrypted.

6. Retention and deletion

Data	Retention
Integration data (creator, order and commission data)	For the duration of the client contract; deleted within 30 days of contract end from n8n (workflow data and executions) and Notion; backups expire under the normal 30-day rotation
n8n execution data	Automatically pruned after 30 days (n8n execution data pruning)
Invoices and accounting records containing commission amounts	As required by German commercial and tax law (HGB, AO)
Restricted data (credentials)	Revoked and deleted when no longer needed, at the latest at contract end

Deletion and correction requests from creators or the seller are handled under the Internal Data Protection Policy. On request, we confirm deletion at contract end to the client in writing.

7. Review

This policy is reviewed annually and whenever a new type of data or a new system is added.