TIKTOK SHOP PARTNER API REVIEW

Information Security and Data Protection Evidence Package

Jinyuandu Trading Co., Ltd.

晋江度**远贸**易有限公司

Prepared for Global Security Office (GSO) reassessment

Document	Information Security and Data Protection Evidence Package
Version	2.0
Policy effective date	6 August 2026
Evidence revision date	12 August 2026
Review cycle	Every six months; next review 6 February 2027
Policy owner	Wang Mingqian
Contact	admin@duyuangmvmax.com
Public evidence index	https://duyuangmvmax.com/data-protection

Purpose of this package

This document supplies the policy documentation and alternative verifiable evidence requested by GSO. It maps every affirmative questionnaire response to a specific policy section or implementation record and clearly identifies controls that are not asserted.

Classification: Internal compliance document shared with TikTok Shop reviewers.

1. Reviewer response and document scope

Response to the rejection

GSO advised that the prior submission lacked evidence of policy documentation or alternative verifiable evidence. Version 2.0 therefore contains the underlying standards, procedures, approval record, live public-policy verification, and application access-control evidence in one indexed package.

Dear TikTok Shop Review Team,

We respectfully submit this revised evidence package for reassessment. It documents the security and privacy controls currently asserted in our questionnaire and provides a page-level cross-reference for each affirmative response. The package includes our information security baseline, access control standard, Personal Information Protection Standard, incident response and notification procedure, data subject request process, retention and deletion procedure, management approval record, and implementation evidence.

Where a control has not been implemented or cannot be evidenced, the questionnaire response remains “No” and the control is not represented as operational. We request that GSO assess the affirmative responses using the matrix in Section 2 and the referenced evidence sections.

Sincerely,
Management Team
Jinyuandu Trading Co., Ltd.

1.1 Scope

- Organization: Jinyuandu Trading Co., Ltd. / 晋江度远贸易有限公司
- System: Duyuan GMV MAX Management Dashboard
- Processing purpose: internal ecommerce operations and authorized TikTok Shop store management
- Data processing/storage region declared in the questionnaire: United States
- Evidence period: current controls and records as of 12 August 2026
- Exclusions: customer data samples, credentials, API secrets, access tokens, and certification claims

1.2 How the reviewer should use this package

1. Locate the questionnaire item in the evidence matrix in Section 2.
2. Confirm that the response shown in the matrix matches the submitted form.
3. Review the cited policy clause and, where applicable, the implementation evidence in Section 10.
4. Use the public URLs in Section 10 to independently verify the published privacy and data-protection pages.

2. Questionnaire-to-evidence matrix

This matrix is the primary reviewer index. “Yes” means the package supplies supporting documentation. “No” means the organization does not assert that control in the current submission.

Questionnaire control	Response	Evidence location	Reviewer note
Published information security strategy or plan	**Yes - update form**	Sections 4-5; approval record in Section 9	Internal Information Security Standard is formally documented and published through the evidence page.
Network isolation and threat monitoring/prevention	**No**	Not asserted	No unsupported implementation claim is made.
Anti-malware installed on company endpoints	**No**	Not asserted	No unsupported implementation claim is made.
Daily operational security baseline	**Yes**	Section 5.1; Appendix A	Mandatory baseline and control verification record.
Access control and least privilege	**Yes**	Sections 5.2-5.5; Section 10.2	Role, store scope, account state, and session invalidation controls.
Data classification and encryption policy	**No**	Section 4.5 is handling guidance only	Do not change to Yes unless encryption-at-rest evidence is available.
Incident response policy	**Yes**	Section 7	Roles, triage, containment, evidence preservation, recovery, and review.
Vulnerability or threat management program	**No**	Not asserted	No unsupported implementation claim is made.
No reportable personal-data breach in past 3 years	**No incidents**	Section 9.3 management attestation	Management record; no contradictory incident record identified.
No regulator/customer data complaint in past 3 years	**No complaints**	Section 9.3 management attestation	Management record; no contradictory complaint record identified.
Internal personal information protection policy	**Yes**	Section 6; approval record in Section 9	Personal Information Protection Standard.
Assist with delete/update/provide-data requests	**Yes**	Section 8.1	Data subject and merchant request procedure.
Privacy policy maintained and periodically updated	**Yes**	Sections 6.8 and 10.1	Live at https://duyuangmvmax.com/privacy.
Designated DPO	**No**	Privacy owner is named; no DPO claim	Responsible administrator coordinates privacy requests.
Suspected/confirmed breach notification process	**Yes**	Sections 7.4-7.6	Defined escalation and external notification workflow.
Delete collected customer data at contract end	**Yes**	Section 8.2	Termination deletion procedure and documented completion record.
ISO 27001 / ISO 27701 / SOC 2 / ePrivacy certification	**No**	Not asserted	No certificate is claimed or attached.

Important form correction

This package supports changing only the first security question to Yes. Keep network isolation, anti-malware, encryption, vulnerability management, DPO, and certification as No unless separately evidenced.

3. Organization, system, and data-flow overview

Legal entity	Jinyuandu Trading Co., Ltd. / 晋江度远贸易有限公司
System	Duyuan GMV MAX Management Dashboard
Business use	Internal ecommerce operations, GMV Max campaign reporting, store performance analysis, and controlled campaign administration
Authorized users	Management and employees assigned to specific stores
External platform	TikTok Shop / TikTok Business API through OAuth authorization
Public website	https://duyuangmvmax.com
Privacy contact	admin@duyuangmvmax.com

3.1 Processing flow

1. An authorized management user initiates TikTok OAuth authorization for a business account or store.
2. TikTok returns authorization credentials to the configured callback. The system uses those credentials to make authorized API requests.
3. The dashboard retrieves store, product, campaign, material, order-performance, and aggregated operational information needed for internal operations.
4. Role and store assignments restrict which stores an employee can see in the dashboard.
5. When authorization is revoked, an account is disabled, or the relationship ends, access is removed and data deletion is initiated under Section 8.

3.2 Data categories

- Store and authorization metadata: store identifiers, advertiser identifiers, authorization status, and business account labels.
- Catalog and campaign data: products, SKUs, GMV Max campaign settings, creative identifiers, and performance reports.
- Order-related operational data: aggregated order metrics and operational status required for fulfillment, reconciliation, reporting, and support.
- Security and operational records: account assignments, audit events, and incident or request records where generated.
- Excluded from this evidence package: API secrets, access tokens, customer records, and raw order data.

3.3 Purpose limitation

TikTok Shop data is processed only for authorized internal ecommerce operations. The organization does not sell, rent, or provide the data to unauthorized third parties and does not use the integration as a public data marketplace.

4. Information Security Standard

Policy owner: Wang Mingqian | Approved by: Management Team | Effective: 6 August 2026 | Review: every six months

4.1 Objective and applicability

This standard establishes minimum administrative and technical safeguards for the organization's internal ecommerce systems and authorized TikTok Shop API processing. It applies to employees, contractors, administrators, endpoints, servers, accounts, and third-party services used to access or process covered data.

4.2 Security principles

- Least privilege: access is limited to the minimum stores and functions required for assigned duties.
- Need-to-know: covered data is not disclosed to staff or third parties without an authorized business purpose.
- Secure authorization: platform access is obtained through approved OAuth or platform authorization flows.
- Accountability: material access, configuration changes, incidents, and deletion actions must be attributable to an owner.
- Data minimization: only the data necessary for the stated operational purpose is accessed or retained.
- Safe change control: production-affecting automation uses confirmation and audit records appropriate to the risk.

4.3 Roles and responsibilities

Management Team	Approves policies, assigns owners, accepts residual risk, and ensures resources for remediation.
Responsible Administrator	Manages accounts and store assignments, coordinates privacy requests and incidents, reviews access, and preserves evidence.
Authorized Employee	Uses only assigned stores, protects credentials, follows the security baseline, and reports suspected incidents immediately.
System Maintainer	Implements approved changes, maintains service configuration, reviews logs, and avoids placing secrets in source control or evidence packages.

4.4 Access authorization lifecycle

1. Management approves the user's role and store scope before account creation.
2. The administrator creates or activates the account and records the assigned stores.
3. Permissions are reviewed at least every six months and when duties change.
4. Accounts are disabled and active sessions invalidated promptly upon termination, role change, credential compromise, or loss of need.

4.5 Data handling rule

Covered TikTok Shop data is treated as Restricted business data. It may be viewed only in approved systems, transmitted only over approved HTTPS connections, and must not be copied into public repositories, public messages, or this evidence package. This handling rule does not constitute a claim that every stored record is encrypted at rest; the questionnaire's separate data-classification/encryption item remains No until verifiable at-rest encryption evidence is available.

5. Security baseline and access control procedures

5.1 Daily operational security baseline

Every endpoint and account used for covered operations must meet the following baseline before access is permitted:

- A password-protected user account and automatic screen lock after no more than 15 minutes of inactivity.
- A strong, unique password; credentials must not be shared or reused across unrelated services.
- Multi-factor authentication enabled where the operating system, hosting provider, email provider, or TikTok account supports it.
- Current security updates installed within the normal vendor-supported update cycle.
- A clean-screen and clean-desktop practice; sensitive information must not be left visible when unattended.
- No storage of TikTok credentials or customer data in personal messaging applications or public cloud folders.
- Immediate reporting of suspicious login prompts, unexpected authorization changes, or lost devices.

Evidence record

The questionnaire includes an endpoint settings screenshot for the daily security baseline. Management must keep the original screenshot attached to the relevant Yes response. This package supplies the governing policy and verification checklist in Appendix A.

5.2 Role-based access model

Super administrator	Authorized management role with visibility across managed stores and responsibility for user/store assignment.
Employee	Operational role limited to the store identifiers assigned to the employee account.
Inactive user	No valid application session; access is denied until reactivated by authorized management.

5.3 Store-level least privilege

Employees must be assigned only to the stores required for their duties. Dashboard store lists and campaign lists are filtered by the user's allowed store identifiers. A user may not use another person's account to reach an unassigned store.

5.4 Session invalidation

When an account is disabled or its password is changed, the application increments the account session version. Existing sessions whose version no longer matches the account record are rejected and the user must authenticate again.

5.5 Access review record

The Responsible Administrator reviews active accounts, roles, and store assignments every six months and after personnel or store-ownership changes. The review records the date, reviewer, exceptions, and remediation completion. Appendix A provides the review form.

6. Personal Information Protection Standard

6.1 Purpose and scope

This standard governs personal information and TikTok Shop data accessed through authorized API integrations and used in the organization's internal ecommerce operations. It applies to all personnel and systems involved in collection, access, use, storage, disclosure, retention, deletion, support, or incident response.

6.2 Lawful and authorized processing

The organization processes data only for stores it owns or is authorized to manage and only for operational purposes supported by the TikTok Shop authorization. Data must not be obtained by bypassing platform permissions or used for unrelated profiling, resale, or unauthorized marketing.

6.3 Collection and minimization

Personnel must request and retain only the data fields needed for the operational function. Debug output, screenshots, and support records must be reviewed to avoid unnecessary customer data or

credentials. Production data must not be copied into development fixtures unless specifically approved and minimized.

6.4 Use and disclosure

Covered data may be used for store monitoring, product management, fulfillment follow-up, campaign and creative performance analysis, operational reporting, reconciliation, and authorized support. Disclosure is restricted to authorized staff, the relevant merchant, TikTok Shop, and service providers necessary to operate the system under appropriate contractual controls.

6.5 Storage location

The current questionnaire states that TikTok Shop data is stored and processed in the United States. Any change to the processing region requires management review and an update to the privacy notice and questionnaire before the change is relied upon.

6.6 Accuracy and correction

Where the system stores operational data, reasonable steps are taken to keep it accurate and current. Authorized correction requests are verified, recorded, and completed through the source platform or internal system as appropriate.

6.7 Individual and merchant rights

Requests to access, correct, provide, restrict, or delete data are handled under Section 8. The organization cooperates with the merchant and TikTok Shop to fulfill verified requests within applicable requirements.

6.8 Transparency and review

The public privacy policy is maintained at https://duyuangmvmax.com/privacy. This standard is reviewed every six months and whenever there is a material change to data categories, purposes, authorization, processing region, platform requirements, or applicable law.

7. Incident response and notification procedure

7.1 Reporting and activation

Any suspected unauthorized access, credential exposure, accidental disclosure, data loss, malware event, unexpected authorization change, or system compromise must be reported immediately to the Responsible Administrator at the internal escalation channel and to the management contact. The administrator opens an incident record and assigns severity.

7.2 Initial response

- Contain: disable affected accounts, revoke authorization, isolate the affected component, or suspend risky automation.
- Preserve: record timestamps, affected accounts/stores, request identifiers, relevant logs, and actions taken without altering original evidence.

- Assess: identify the data categories, number of affected records or stores, duration, cause, recipients, and likelihood of harm.
- Eradicate and recover: remove the cause, rotate credentials where applicable, restore safe operation, and verify the control before resuming processing.

7.3 Severity

Critical	Confirmed credential or customer-data compromise, active unauthorized access, or material platform impact. Immediate management escalation.
High	Likely compromise or significant control failure with limited confirmation. Contain immediately and investigate continuously.
Medium	Contained event with limited exposure or unsuccessful unauthorized activity. Investigate and remediate promptly.
Low	Policy deviation or suspicious event with no identified exposure. Record, correct, and monitor.

7.4 External notification decision

Management determines whether notification is required to TikTok Shop, the affected merchant, individuals, service providers, or regulators based on confirmed facts, platform terms, contractual commitments, and applicable law. The decision and rationale are recorded even when notification is not required.

7.5 Notification content and timing

When notification is required, it is made without undue delay after sufficient facts are available. The notice includes the nature and timing of the incident, affected data and stores, containment actions, current risk, recommended protective steps, point of contact, and planned updates. Unverified speculation and secrets are excluded.

7.6 Post-incident review

After recovery, management records root cause, corrective actions, owners, completion dates, residual risk, and any required policy or questionnaire update. Access assignments and affected credentials are revalidated before closure.

8. Data requests, retention, and deletion

8.1 Request handling procedure

1. Receive the request through admin@duyuangmvmax.com, the merchant, or TikTok Shop and create a request record.
2. Verify the requester’s authority and define the store, person, data, and requested action.

3. Locate relevant records in approved systems and identify any legal, security, or platform restriction.
4. Provide, correct, export, restrict, or delete the data as authorized; coordinate with TikTok Shop or the merchant when the source platform must perform the action.
5. Document completion, exceptions, communications, date, and responsible person. Do not place unnecessary personal data in the request log.

8.2 Contract termination and authorization revocation

1. Disable user and store access and stop scheduled processing for the affected relationship.
2. Revoke or delete locally held authorization credentials and confirm that no active job continues to use them.
3. Delete or anonymize locally retained customer and store data that is no longer required, subject to documented legal, dispute, or audit obligations.
4. Record the systems checked, deletion method, exceptions, approver, and completion date.
5. Notify the merchant or TikTok Shop of completion when requested or contractually required.

8.3 Retention schedule

Record category	Operational retention rule	Deletion trigger	Exception
OAuth credentials	**Only while authorization and business need remain**	Revocation, replacement, expiry, or relationship end	None beyond technical completion needs
Store/campaign operational data	**Only while needed for authorized operations and reporting**	No business need or relationship end	Documented legal, dispute, or audit hold
Audit and execution records	**Long enough to investigate changes and demonstrate accountability**	End of approved audit period	Active incident, legal, or dispute hold
Incident/request records	**Until closure plus the approved compliance retention period**	Retention period expires	Legal or regulatory requirement
Backups	**Normal backup lifecycle; not used as an active archive**	Backup expiry or secure overwrite	Recovery integrity requirements

Deletion assurance

A deletion is not complete until the responsible administrator records the systems checked, remaining exceptions, and completion date. Data under a valid hold is access-restricted and deleted when the hold ends.

9. Governance, approval, and compliance records

9.1 Document control and approval record

Policy set	Information Security Standard; Personal Information Protection Standard; Incident Response and Notification Procedure; Data Request, Retention, and Deletion Procedure
Owner / responsible person	Wang Mingqian
Approval authority	Management Team
Original effective date	6 August 2026
Current evidence version	2.0
Revision date	12 August 2026
Review frequency	At least every six months and upon material change
Next scheduled review	6 February 2027
Approval status	Approved for internal operational use and external compliance evidence

9.2 Revision history

Version	Date	Change	Approved by
1.0	**6 Aug 2026**	Initial Personal Information Protection Standard and data protection package	Management Team
2.0	**12 Aug 2026**	Added security standard, page-level evidence matrix, incident notification procedure, deletion workflow, implementation evidence, and reviewer instructions	Management Team

9.3 Management attestation

Based on management records available as of the revision date:

- The organization is not aware of a reportable security breach in the preceding three years that caused accidental or unlawful exposure of personal data and required notification to a government authority, regulator, affected customer, or individual.
- The organization is not aware of a data-protection regulator notice or customer/individual complaint in the preceding three years concerning its processing of personal data.
- The organization has not obtained ISO 27001, ISO 27701, SOC 2 Type 2, ePrivacy, or a comparable certification and does not represent otherwise.

Attestation owner: Management Team | Responsible person: Wang Mingqian | Record date: 12 August 2026

9.4 Review checklist

- Confirm questionnaire answers still match implemented and evidenced controls.
- Review active users, roles, store assignments, and disabled accounts.
- Confirm the public privacy and data-protection URLs remain available and current.
- Review incidents, requests, complaints, retention exceptions, and outstanding remediation.
- Review changes to TikTok scopes, data fields, storage region, subprocessors, and automation.
- Approve the updated version and record the next review date.

10. Verifiable implementation evidence

10.1 Public policy verification

Privacy policy	https://duyuangmvmax.com/privacy
Data protection evidence index	https://duyuangmvmax.com/data-protection
Downloadable package	https://duyuangmvmax.com/data-protection-compliance.pdf
Verification performed	12 August 2026
Observed HTTP result	200 OK for the privacy policy page
Observed page title	Privacy Policy | Duyuan GMV MAX Management Dashboard
Published company/contact	Jinyuandu Trading Co., Ltd.; admin@duyuangmvmax.com

Independent verification

The reviewer can open the URLs above without access to the internal dashboard. The public privacy page identifies the company, processing purposes, United States storage region, role-based access control, security measures, retention/deletion commitments, and the downloadable compliance package.

10.2 Application access-control evidence

Evidence A - role and store-scope data model

Source: src/automation.ts:32-40 and 230-236 | repository commit 4348d1b

```
export interface UserAccount {
  role: UserRole;
  sessionVersion?: number;
  storeIds: string[];
  active: boolean;
```

```
}
export function visibleStoreIds(user, stores) {
  if (user.role === "super_admin") return stores.map((store) => store.id);
  return user.storeIds;
}
```

This data model distinguishes role, account status, session version, and assigned store identifiers. Super administrators receive management visibility; employee visibility is derived from explicit store assignments.

Evidence B - session validity and store filtering

Source: src/App.tsx:685-688 and 866-869 | repository commit 4348d1b

```
const currentUser = users.find((user) => {
  const version = Number(user.sessionVersion || 0);
  return user.id === session.userId && user.active
    && version === session.sessionVersion;
});
const allowedStoreIds = visibleStoreIds(currentUser, stores);
const visibleStores = stores.filter((store) =>
  allowedStoreIds.includes(store.id));
const scopedCampaigns = campaigns.filter((campaign) =>
  allowedStoreIds.includes(campaign.storeId));
```

An inactive account or stale session version is not accepted as the current user. Stores and campaigns are scoped through the allowed-store list before display.

Evidence C - password/status change invalidates sessions

Source: src/App.tsx:3561-3569 and 3668-3669 | repository commit 4348d1b

```
const shouldInvalidateSession = passwordChanged || statusChanged;
sessionVersion: shouldInvalidateSession
  ? Number(user.sessionVersion || 0) + 1
  : user.sessionVersion,
storeIds: user.role === "super_admin" ? [] : draft.storeIds,
// UI notice: changing a password or disabling an account
// invalidates existing sessions and requires re-authentication.
```

The application invalidates existing sessions when a password is changed or an account is disabled, and it preserves explicit employee store assignments.

10.3 OAuth authorization evidence

Evidence D - anti-forgery state and session cleanup

Source: server/tiktokOAuth.mjs:150-174 and 177-218 | repository commit 4348d1b

```
pruneSessions();
const state = randomBytes(16).toString("hex");
oauthSessions[state] = { ... , createdAt: Date.now() };
authUrl.searchParams.set("state", state);
...
const session = oauthSessions[state];
if (!session) throw new Error("OAuth state is invalid or expired");
...
delete oauthSessions[state];
```

The authorization flow creates a random OAuth state, rejects missing or expired state, and removes the one-time session after completion. Secrets and token values are intentionally excluded from this evidence.

Appendix A - control verification records

A.1 Daily security baseline verification

Control	Expected evidence	Result / reference	Owner

Control	Expected evidence	Result / reference	Owner
Automatic screen lock	**Endpoint settings screenshot showing inactivity lock**	Original screenshot attached to questionnaire	Responsible Administrator
Password-protected account	**Endpoint sign-in/security settings or management confirmation**	Verify before submission	Responsible Administrator
Strong unique password	**Management attestation; do not attach password values**	Verify before submission	Account owner
MFA where available	**Provider security page or account settings screenshot**	Attach only if enabled	Account owner
Security updates	**Operating-system update status**	Verify during access review	Account owner
Clean-screen practice	**Policy acknowledgement**	Covered by Section 5.1	All authorized users

Verification date: _____ Reviewer: _____ Exceptions/remediation: _____

A.2 Access review record

User / role	Assigned stores	Active?	Business need confirmed?	Remediation / date
_____	_____	Yes / No	Yes / No	_____
_____	_____	Yes / No	Yes / No	_____
_____	_____	Yes / No	Yes / No	_____

Review date: _____ Reviewer: _____ Next review: _____

A.3 Incident / notification record

Incident ID and discovery time	_____
Affected stores, systems, and data	_____
Containment and evidence preserved	_____
Notification decision and basis	_____
Recipients and notification	_____

time	
Root cause and corrective actions	_____
Owner and closure approval	_____

Appendix B - submission checklist and exact text

B.1 Files and links to submit

- Upload the final PDF version of this package to every affirmative questionnaire item that offers an attachment field, especially daily security baseline, access control, incident response, internal personal data protection policy, and breach notification process.
- Keep the original endpoint settings screenshot attached to the daily security baseline question.
- Use https://duyuangmvmax.com/privacy in the privacy-policy binding field.
- Do not upload ISO/SOC certificates because the certification response is No.
- Do not change network isolation, anti-malware, data classification/encryption, vulnerability management, or DPO to Yes without separate evidence.
- After deployment, verify that the public compliance PDF URL opens successfully in a private/incognito browser window.

B.2 Recommended English explanations

Information security strategy	Our organization has adopted and published an internal Information Security Standard covering least privilege, account lifecycle, endpoint security baseline, secure authorization, incident response, and six-month reviews. The attached v2.0 Evidence Package contains the approved policy and implementation evidence.
Daily security baseline	Our daily security baseline requires password-protected endpoints, automatic screen lock after no more than 15 minutes of inactivity, strong unique passwords, MFA where available, current security updates, and clean-screen practices. The attached package contains the policy and verification record.
Access control	Access is restricted to authorized internal personnel using role-based and store-level access control. Employee accounts can access only assigned stores. Disabled accounts and sessions invalidated by password or status changes cannot remain active. See Sections 5 and 10 of the attached package.
Incident response	Our documented incident response procedure defines reporting, severity, containment, evidence preservation, investigation, recovery, notification assessment, corrective actions, and post-incident review. See Section 7 of the attached package.
Personal data protection policy	Our approved Personal Information Protection Standard covers authorized processing, data minimization, purpose limitation, United States processing location, access control, data requests, retention, deletion, incident response, and six-month policy review. See Sections 6-9 of the attached package.

Breach notification	Suspected incidents are escalated immediately. Management assesses whether TikTok Shop, the merchant, individuals, service providers, or regulators must be notified and records the decision. Required notices are sent without undue delay with confirmed facts and remediation steps.
Contract termination deletion	At relationship end we disable access, stop processing, revoke locally held authorization credentials, delete or anonymize data no longer required, document any legal hold, and record completion. See Section 8.2 of the attached package.

B.3 Recommended reviewer note

Paste into the Notes field

Dear TikTok Shop Review Team, in response to the GSO request for evidence, we have attached our revised Information Security and Data Protection Evidence Package v2.0. The package contains a page-level questionnaire evidence matrix, approved security and personal information protection standards, access control requirements and implementation excerpts, incident response and notification procedures, data request and deletion procedures, management approval records, and independently verifiable public policy URLs. Controls not implemented or not evidenced remain marked No. Please use Section 2 as the reviewer index and reassess our application. Thank you.

B.4 Final consistency check

- Every Yes response has an English explanation and an attachment or a precise reference to this package.
- The policy URL is exactly https://duyuangmvmax.com/privacy (not /privacy-policy).
- The company name, website, contact email, processing region, effective date, and review cycle match across the form, website, and package.
- No answer claims a certification, DPO, anti-malware deployment, network isolation, encryption-at-rest implementation, or vulnerability program without evidence.
- The uploaded PDF opens, has searchable text, and contains no passwords, access tokens, customer data, or API secrets.

End of evidence package