BIGVIRALS

PERSONAL DATA PRIVACY PROGRAM AND HANDLING POLICY

Internal rules for collecting, using, storing, transmitting, sharing, retaining, and deleting personal data

Legal Entity / TikTok Shop Developer	江西省深蓝智科文化有限公司
Service Brand	BIGVIRALS
Application	bigvirals-Creator Outreach
Official Website	https://www.bigvirals.com/
Public Privacy Policy	https://www.bigvirals.com/privacy.html
Privacy Contact	support@bigvirals.com
Version	1.0
Effective Date	July 12, 2026
Review Cycle	At least annually and after material business, system, legal, platform, privacy, or security changes
Document Status	Approved internal privacy program and handling baseline

Entity and brand clarification

江西省深蓝智科文化有限公司 is the legal entity, TikTok Shop developer, and operator of the Services. BIGVIRALS is a product and service brand operated by the Company and is not a separate legal entity. bigvirals-Creator Outreach is the TikTok Shop application operated by the same Company.

Approved by: Management of 江西省深蓝智科文化有限公司

Approval Date: July 12, 2026

Document Control

Policy Owner	Privacy Lead designated by Company Management
Accountable Executive	Company Management
Applies To	Employees, contractors, temporary personnel, systems, applications, devices, APIs, cloud services, service providers, and business processes used for BIGVIRALS operations
Primary Data Domains	Merchant, seller, creator, contact, collaboration, campaign, authentication, technical, operational, support, billing, and platform data
Review Frequency	At least once every 12 months and whenever a material change, high-risk processing activity, significant privacy incident, or applicable requirement occurs
Exception Authority	Company Management or its formally delegated Privacy Lead
Availability	Internal policy that may be shared with TikTok Shop, merchants, auditors, regulators, and other authorized reviewers

Revision History

Version	Date	Owner	Summary
1.0	July 12, 2026	Company Management	Initial comprehensive privacy program covering governance and the full personal-data lifecycle, including collection, storage, transfer, sharing, rights handling, retention, and deletion.

Policy Statement

江西省深蓝智科文化有限公司 (the "Company") is committed to handling personal data lawfully, fairly, transparently, securely, and only for legitimate business and service purposes. This policy establishes the mandatory privacy baseline for BIGVIRALS and the bigvirals-Creator Outreach application.

The Company will maintain a documented privacy program, assign accountability, keep records of processing activities, minimize data collection, control access, manage service providers, respond to privacy requests, delete data when no longer needed, and review the effectiveness of this program on a recurring basis.

Minimum operating rule

No personal data may be collected, accessed, used, exported, transmitted, shared, retained, or deleted outside an approved business purpose, authorized workflow, and documented control process.

Policy Structure

Lifecycle Stage	Primary Controls
Govern	Ownership, inventory, risk assessment, approval, training, audit, evidence
Collect	Notice, authorization, purpose definition, minimization, accuracy
Use	Purpose limitation, role-based access, confidentiality, monitoring
Store	Approved systems, security controls, location awareness, backups
Transfer / Share	Need-to-know, minimum data, secure channel, contract, record
Retain / Delete	Retention schedule, deletion queue, backups, verification
Respond	Rights requests, authorization revocation, complaints, incidents

1. Purpose and Objectives

This policy establishes an organization-wide privacy program for the proper handling of personal data throughout its lifecycle. Its objectives are to:

- Protect individuals, merchants, sellers, creators, users, business partners, and platform participants from privacy harm.
- Ensure personal data is collected and processed only for specified, legitimate, and authorized purposes.
- Define consistent rules for collection, use, storage, access, transmission, sharing, retention, and deletion.
- Enable the Company to demonstrate accountability through records, approvals, logs, training, reviews, and evidence.
- Align BIGVIRALS operations with applicable laws, contracts, user authorizations, and TikTok Shop requirements.

2. Scope

This policy applies to all personal data and platform data handled by or on behalf of the Company, whether stored electronically, in paper form, in cloud systems, on endpoints, in communication tools, in backups, or through third-party services.

Covered people and resources

- Employees, contractors, consultants, interns, temporary personnel, and authorized representatives.
- BIGVIRALS websites, applications, databases, APIs, scripts, cloud services, file stores, devices, communication channels, and support systems.
- Service providers, processors, sub-processors, hosting providers, payment providers, analytics providers, professional advisers, and other recipients that process data for the Company.

Covered data

- Business contact and account data; merchant, seller, shop, creator, campaign, collaboration, support, billing, and operational data.
- Authentication data, API authorization data, access tokens, logs, device and network information, and identifiers.
- Any information that identifies, relates to, describes, can reasonably be linked with, or could be used to distinguish an individual.

3. Definitions

Personal Data	Information relating to an identified or identifiable individual, including direct and indirect identifiers.
Processing	Any operation performed on data, including collection, recording, organization, use, access, analysis, storage, transmission, sharing, retention, deletion, or destruction.
Data Subject	The individual to whom personal data relates.
Sensitive Data	Personal data requiring enhanced protection because misuse could create significant harm, including credentials, government identifiers, financial details, precise location, health data, biometric data, and data concerning minors.
Controller / Business	The party that determines why and how personal data is processed.
Processor / Service Provider	A party that processes personal data on behalf of another party and according to documented instructions.
Privacy Incident	A suspected or confirmed event involving unauthorized collection, access, use, disclosure, alteration, loss, or deletion of personal data.
Deletion	Removal or irreversible de-identification of data so it is no longer available for routine use or linked to an individual.

4. Privacy Principles

Principle	Required Outcome
Lawfulness, fairness, and transparency	Process data only under an authorized and appropriate basis; provide clear information about processing.
Purpose limitation	Define the purpose before collection and do not use data for incompatible or unrelated purposes.
Data minimization	Collect and retain only the minimum data reasonably necessary for the approved purpose.
Accuracy	Take reasonable steps to keep data accurate, complete, and current for its intended use.
Storage limitation	Do not retain identifiable data longer than necessary for business, legal, contractual, security, or platform needs.
Integrity and confidentiality	Protect data using appropriate administrative, technical, and organizational safeguards.
Accountability	Assign ownership, document decisions, maintain evidence, review effectiveness, and correct deficiencies.

5. Privacy Governance and Accountability

5.1 Management responsibilities

- Approve this policy and provide reasonable resources for privacy compliance.
- Designate a Privacy Lead and define authority to investigate, stop, or escalate non-compliant processing.
- Review significant privacy risks, incidents, exceptions, and remediation plans.
- Ensure business objectives do not override mandatory privacy and platform obligations.

5.2 Privacy Lead responsibilities

- Maintain this policy, the data inventory, records of processing, retention schedule, vendor register, and privacy evidence.
- Coordinate privacy reviews for new systems, APIs, products, data sources, vendors, markets, and processing purposes.
- Manage data-subject requests, complaints, deletion requests, and authorization-revocation workflows.
- Coordinate with Information Security on access control, incident response, logging, testing, and remediation.
- Provide training, conduct periodic reviews, report metrics, and escalate significant risks to Management.

5.3 Business and system owners

- Document the purpose, data categories, source, recipients, storage location, access roles, and retention period for their processing activities.
- Ensure only approved personnel and systems process data and that access is removed when no longer needed.
- Complete privacy reviews before materially changing a workflow or repurposing data.
- Cooperate with access, correction, deletion, audit, and incident-response requests.

5.4 Personnel responsibilities

- Use personal data only for assigned duties and approved purposes.
- Do not copy data to personal accounts, unapproved devices, personal cloud drives, public AI tools, or unauthorized communication channels.
- Report suspected privacy incidents, incorrect data, excessive access, or inappropriate sharing immediately.
- Complete required training and comply with confidentiality obligations during and after engagement with the Company.

6. Data Inventory and Records of Processing

The Company will maintain a practical data inventory and record of processing activities for systems and workflows that handle personal data. The record must be sufficient to show what data is processed, why, where, by whom, for how long, and with whom it is shared.

Required Record Field	Minimum Detail
Processing activity	Business process, system, feature, integration, or service
Purpose	Specific operational, contractual, security, compliance, or support purpose
Data categories	Identifiers, contact data, creator data, account data, logs, tokens, support records, etc.
Data subjects	Merchants, sellers, creators, users, representatives, employees, applicants, or others
Source and collection method	Direct input, authorized API, customer submission, public source, system-generated
System and storage location	Application, database, cloud environment, file store, support tool, backup
Access roles	Job functions and service accounts with access
Recipients and vendors	Internal teams, platforms, processors, advisers, authorities
Retention and deletion	Retention trigger, active period, deletion method, backup treatment
Risk and controls	Sensitivity, cross-border issues, security controls, review status

Inventory update trigger

The inventory must be updated before a new collection, new data category, new recipient, new vendor, new API scope, new country, new automated use, or material change is put into production.

7. Collection and Privacy Notice

7.1 Pre-collection requirements

Before collecting personal data, the responsible owner must document and obtain approval for:

- The specific purpose and expected business outcome.
- The minimum data elements required and why each element is necessary.
- The data source and whether the source is authorized, reliable, and appropriate.
- The applicable notice, consent, contract, platform authorization, or other processing condition.
- The intended users, systems, recipients, storage location, retention period, and deletion method.
- Any sensitive-data, minor, international-transfer, automated-processing, or platform-specific risk.

7.2 Notice and transparency

- Provide a clear privacy notice at or before collection where required and reasonably practical.
- Describe the legal entity, service, categories of data, purposes, recipients, retention approach, rights, and contact method.
- Do not use vague language to conceal unrelated, unexpected, or excessive processing.
- Keep the public Privacy Policy aligned with actual processing and update it before material new uses begin.

7.3 Collection channels

Personal data may be collected only through approved channels such as account forms, service interfaces, authorized platform APIs, customer-support channels, signed agreements, approved business communications, or other documented sources. Web scraping, bulk extraction, or collection outside platform rules is prohibited unless specifically approved and lawful.

8. Authorization and Lawful Processing

Each processing activity must have an authorized basis appropriate to the relevant context. Depending on the activity and applicable requirements, this may include user consent, platform authorization, performance of a contract, a legitimate and balanced business need, compliance with a legal obligation, or protection of rights and security.

Authorization controls

- Authorization must be specific enough to support the intended data and function.
- API scopes and permissions must be limited to what the service actually uses.
- Authorization status, scope, time, account, and revocation must be recorded where technically available.
- Processing must stop when authorization expires or is revoked, except for limited deletion, security, dispute, or legally required retention activities.
- Consent must not be bundled with unrelated purposes where separate choice is required.

9. Data Minimization and Accuracy

9.1 Minimization rules

- Do not collect data merely because it may be useful in the future.
- Avoid free-text fields when structured fields can reduce unnecessary personal information.
- Do not collect sensitive data unless specifically approved, necessary, and protected by enhanced controls.
- Use aggregated, masked, tokenized, or de-identified data when individual-level information is not required.
- Limit exports, reports, logs, test datasets, and screenshots to the minimum information needed.

9.2 Accuracy rules

- Provide reasonable methods for authorized users and individuals to correct material inaccuracies.
- Correct or delete information that is confirmed inaccurate and could affect decisions or services.
- Record the source and update time where accuracy is important.
- Propagate material corrections to relevant downstream systems or recipients where reasonably necessary.

10. Use and Purpose Limitation

Personal data may be used only for the documented purpose or a compatible, authorized purpose. Before using data for a materially different purpose, the owner must complete a privacy review and, where required, update the notice, obtain authorization, amend contracts, or collect new consent.

Prohibited uses

- Unauthorized profiling, surveillance, discrimination, harassment, spam, or manipulation.
- Selling, renting, trading, or disclosing TikTok Shop data or personal data to unrelated parties.
- Using personal data to train public or third-party AI systems without documented approval, appropriate terms, and necessary authorization.
- Using creator or merchant data for unrelated advertising or enrichment outside the approved service purpose.
- Attempting to re-identify data that has been intentionally anonymized or de-identified.

11. Storage and Security of Personal Data

Personal data must be stored only in approved systems that are appropriate to the sensitivity, purpose, and operational risk of the data. The Company will coordinate privacy and information-security controls so that confidentiality, integrity, availability, and deletion requirements can be met.

11.1 Storage requirements

- Use approved business accounts, managed databases, cloud storage, and file repositories.
- Prohibit routine storage in personal email, personal messaging accounts, personal cloud drives, removable media, or local downloads unless specifically approved.
- Apply access controls, authentication, logging, secure configuration, patching, backups, and recovery measures appropriate to the system.
- Use encryption in transit through secure protocols and encryption at rest where supported and appropriate.
- Separate production data from development and testing environments. Use synthetic or de-identified test data wherever practical.
- Document the country or region of primary storage and any remote access locations for regulated or platform data.

11.2 Credentials, tokens, and secrets

- Passwords, API keys, client secrets, access tokens, refresh tokens, and encryption keys must not be stored in source code, public repositories, tickets, screenshots, or unapproved documents.
- Secrets must be restricted to authorized systems and personnel and rotated or invalidated after compromise, expiration, revocation, or role change.
- Logs must avoid recording complete tokens, passwords, or unnecessary personal data.

12. Access Control and Internal Handling

12.1 Need-to-know and least privilege

- Grant access only to personnel who require the data for an approved job responsibility.
- Use role-based access where practical and avoid shared accounts.
- Require management or system-owner approval for privileged, bulk-export, administrative, or sensitive-data access.
- Review access periodically and promptly remove access after termination, transfer, contract completion, or loss of business need.
- Use multi-factor authentication where available for administrative, cloud, source-code, email, and data-access accounts.

12.2 Operational handling rules

Activity	Required Handling
Viewing	Use approved systems; prevent shoulder-surfing and unauthorized screen sharing.
Copying / export	Export only when necessary; minimize columns and rows; record high-risk or bulk exports.
Email / messaging	Verify recipients; use approved business channels; avoid unnecessary attachments.
Screenshots	Capture only necessary content; redact unrelated identifiers; delete after the purpose is complete.
Printing	Avoid unless required; retrieve immediately; store securely; shred when no longer needed.
Remote work	Use approved devices, protected networks, screen lock, and secure access methods.
Support access	Use time-limited or case-specific access where practical; record actions and close access after resolution.

High-risk action rule

Bulk exports, unrestricted database access, access to tokens or credentials, sensitive-data handling, and transfers outside the approved environment require elevated approval and evidence of business need.

13. Transmission and Secure Transfer

Personal data may be transmitted only through approved, secure, and purpose-appropriate channels. The sender is responsible for confirming the recipient, minimizing the data, applying safeguards, and recording the transfer where required.

13.1 Transfer checklist

- Confirm the recipient identity, authority, and business need.
- Confirm that the transfer is consistent with the notice, authorization, contract, law, and platform requirements.
- Remove unnecessary fields, records, attachments, and metadata.
- Use secure APIs, encrypted web connections, approved file-sharing tools, or other protected channels.
- Use access expiration, passwords delivered through a separate channel, download restrictions, or encryption where appropriate.
- Retain a record of high-risk, recurring, cross-border, bulk, or externally shared transfers.

13.2 Prohibited transfer methods

- Personal email accounts, personal cloud storage, public links without access control, unapproved consumer messaging apps, or unencrypted removable media.
- Copying data into public AI tools, public code repositories, public issue trackers, or public collaboration spaces.
- Sending full datasets where a summary, token, masked field, or limited record would meet the purpose.

14. Sharing and Disclosure

Personal data may be shared only with authorized internal teams, customers, platforms, service providers, professional advisers, or authorities when the sharing is necessary, proportionate, documented, and protected.

Sharing Requirement	Mandatory Control
Purpose	Specific, legitimate, documented, and consistent with the original collection or a newly authorized purpose
Recipient	Identity, role, authority, and need-to-know verified
Minimum data	Only the fields and records required for the purpose
Terms	Contract, confidentiality obligation, platform terms, or lawful authority as applicable
Security	Appropriate access control, transmission protection, storage, incident, and deletion obligations
Record	Recipient, date, purpose, data categories, approval, and transfer mechanism recorded where material
Follow-up	Correction, deletion, revocation, or incident instructions communicated when applicable

15. Service Provider and Third-Party Management

15.1 Due diligence before access

- Assess the provider’ s services, data access, storage and access locations, security measures, sub-processors, incident history, and ability to support deletion and privacy requests.
- Confirm the provider will use data only for documented services and will not sell, combine, or independently exploit the data.

- Use written terms addressing confidentiality, security, instructions, sub-processing, incident notification, assistance with rights, retention, deletion, audit, and return of data.
- Apply a risk-based review appropriate to the volume, sensitivity, and platform restrictions of the data.

15.2 Ongoing oversight and exit

- Review material providers periodically and when services, ownership, sub-processors, locations, or risks materially change.
- Maintain a vendor register with owner, purpose, data categories, contract status, location, review date, and termination requirements.
- At termination, disable access and obtain deletion or return confirmation where appropriate.

16. International Transfers and Data Location

Before personal data is stored, accessed, or transferred across countries or regions, the owner must confirm that the transfer is permitted by applicable law, contract, platform rules, and the user’ s authorization. Where required, the Company will implement contractual safeguards, data-location controls, encryption, access restrictions, or other approved measures.

Platform data rule

TikTok Shop data may be stored, accessed, transmitted, and processed only in locations and by recipients permitted by the relevant TikTok Shop requirements, API permissions, and agreements.

17. Retention, Deletion, and Disposal

The Company will retain identifiable personal data only for as long as reasonably necessary for the documented purpose and any legitimate legal, contractual, accounting, security, dispute, or platform requirement. Each material processing activity must have a retention trigger and disposal method.

17.1 Retention rules

- Unless a different period is required by law, contract, security needs, or TikTok Shop instructions, platform data associated with a revoked authorization or terminated service should be deleted or irreversibly de-identified from active systems within 30 days; protected backup copies should expire through the normal backup cycle, targeted at no more than 90 days.
- Retention periods must be tied to the purpose, account or contract status, authorization status, legal need, or operational event.
- Indefinite retention is prohibited unless the data is irreversibly de-identified or a documented legal requirement applies.
- Retention schedules must cover primary systems, exports, support tools, logs, collaboration records, temporary files, and backups.
- Owners must periodically review whether data can be deleted, aggregated, or de-identified earlier.
- Legal holds or active investigations may temporarily suspend deletion for specifically identified records.

17.2 Deletion triggers

- Expiration of the documented retention period.
- Closure or deletion of the BIGVIRALS account, subject to necessary residual obligations.
- Termination of the customer, merchant, creator, partner, or service-provider relationship.
- Revocation or expiration of platform authorization or API access.
- Approved deletion request from the individual, customer, controller, or platform.
- Determination that the data is excessive, inaccurate, unlawfully obtained, or no longer needed.

17.3 Deletion methods

Data Location	Approved Deletion / Disposal Method
Application / database	Logical deletion followed by permanent deletion, record-level erasure, or irreversible de-identification according to the system design
Files and exports	Delete from approved storage, recycle bins, shared links, local copies, and temporary folders
Cloud and SaaS tools	Use provider deletion functions and, for material datasets, record confirmation or evidence
Tokens and credentials	Revoke, invalidate, rotate, and remove from active stores and caches
Devices and media	Secure erase, cryptographic erase, managed wipe, or approved physical destruction
Paper records	Cross-cut shredding or approved confidential-disposal service
Backups	Expire or overwrite through the documented backup cycle; prevent restoration to routine use after deletion

17.4 Deletion verification

- Deletion requests and scheduled deletion jobs must be tracked to completion.
- Material deletion actions must record the requester or trigger, systems searched, action taken, date, owner, exceptions, and verification result.

- If deletion cannot be completed, the data must be restricted from routine use and the reason, authority, and revised date documented.
- When restored from backup, previously deleted records must not be returned to active use unless a lawful and authorized reason exists.

18. Data Subject Requests and Privacy Complaints

The Company will provide a documented process for receiving, verifying, tracking, fulfilling, and responding to privacy requests. Rights vary by jurisdiction and relationship; requests will be handled according to applicable requirements and contractual roles.

18.1 Supported request types

- Access or confirmation of processing.
- Correction of inaccurate or incomplete personal data.
- Deletion or erasure.
- Restriction or objection to certain processing.
- Withdrawal of consent or revocation of authorization.
- Data portability where applicable and technically feasible.
- Opt-out from non-essential marketing communications.
- Complaint, appeal, or concern about collection, use, sharing, or retention.

18.2 Request workflow

1. Receive and log the request, channel, date, requester, and scope.
2. Verify identity or authority using proportionate information; do not collect excessive verification data.
3. Clarify scope where necessary and determine the Company’ s role as controller, processor, or service provider.
4. Search relevant systems, vendors, and records; place temporary restrictions where appropriate.
5. Review legal, security, fraud, contractual, and third-party rights exceptions.
6. Complete the action, record evidence, and communicate the result within the applicable timeframe.
7. Notify relevant recipients or business customers of correction, deletion, or restriction where required.

19. Consent, Authorization, and Revocation

- Consent and platform authorization records must be linked to the relevant account, purpose, scope, and time where practical.
- Withdrawing consent or revoking authorization must be as accessible as granting it where required.
- After revocation, new collection and API access under that authorization must stop promptly.
- Residual data must be deleted, de-identified, or restricted according to Section 17, subject to documented exceptions.
- Revocation of TikTok Shop authorization does not automatically delete a separate BIGVIRALS account; account deletion is handled through the applicable account or privacy-request process.

20. TikTok Shop API and Platform Data Handling

The bigvirals-Creator Outreach application may process TikTok Shop data only through approved APIs, approved scopes, authorized accounts, and permitted business functions. TikTok Shop data is subject to this policy plus applicable TikTok Shop developer, privacy, security, and platform requirements.

20.1 Mandatory controls

- Request and use only scopes needed for disclosed creator-outreach, collaboration, campaign, and related support functions.
- Validate authorization before API access and stop access after revocation, expiration, account disconnection, or platform instruction.
- Protect client credentials, tokens, identifiers, responses, and logs from unauthorized access or disclosure.
- Do not sell, rent, trade, scrape beyond authorized functionality, or disclose TikTok Shop data to unrelated parties.
- Do not combine TikTok Shop data with unrelated datasets for unauthorized profiling, advertising, enrichment, or surveillance.
- Limit human access and bulk export; log or approve elevated access where practical.
- Comply with platform data-location, retention, deletion, incident-notification, audit, and cooperation requirements.

20.2 Merchant, seller, and creator data

Merchant, seller, shop, creator, product-collaboration, invitation, campaign, performance, and communication information may be processed only when available through approved functionality or lawfully provided by an authorized party, and only to deliver the disclosed service.

21. Sensitive Data and Children

21.1 Sensitive data

The Services are not designed to routinely collect government identifiers, complete payment credentials, biometric data, medical data, precise real-time location, or other highly sensitive information. Such collection is prohibited unless specifically necessary, approved, lawfully authorized, and protected by enhanced controls.

21.2 Minors

- BIGVIRALS business accounts are intended for adults and authorized business representatives.
- Personnel must not knowingly collect personal data directly from children through BIGVIRALS registration or outreach workflows without a documented, lawful, and approved basis.
- If information relating to a minor is identified, access and use must be limited, applicable platform rules must be followed, and the Privacy Lead must determine whether deletion or additional safeguards are required.

22. Cookies, Analytics, and Tracking

The Company may use cookies, local storage, logs, and similar technologies for authentication, security, preferences, service operation, diagnostics, and analytics. Non-essential tracking must be assessed for notice, consent, opt-out, vendor, retention, and cross-context advertising implications before use.

Technology Category	Privacy Rule
Essential	May be used for login, session, security, load balancing, and core functionality.
Preferences	Use only to remember user-selected settings and provide appropriate controls.
Analytics	Minimize identifiers, limit retention, configure vendors to avoid unrelated use, and obtain consent where required.
Advertising / cross-context	Not permitted without specific Management and Privacy Lead approval, clear notice, applicable choice, and documented legal review.

23. Privacy by Design and Change Management

Privacy requirements must be considered before development, procurement, configuration, or launch of systems and processing activities. Privacy review is part of the Company’ s product, API, vendor, and operational change process.

23.1 Privacy review triggers

- New product, feature, application, API, endpoint, scope, integration, or data source.
- New sensitive-data category, automated decision, profiling use, or high-volume dataset.
- New vendor, sub-processor, storage region, transfer location, or recipient.
- New purpose, marketing use, AI use, public-data collection, or data combination.
- Material change to retention, deletion, security, access, or user choice.
- Processing that may create a high risk to individuals, merchants, creators, or platform participants.

23.2 Privacy impact review

Review Question	Expected Evidence
What is the purpose?	Written purpose, owner, expected benefit, and necessity
What data is involved?	Data categories, subjects, source, sensitivity, and volume
Can less data be used?	Minimization decision, masking, aggregation, or alternative design
Who can access or receive it?	Roles, vendors, locations, contracts, and permissions
What could harm individuals?	Risk scenarios, likelihood, impact, and affected groups
How is risk reduced?	Technical, organizational, contractual, and user-control measures
How is data deleted?	Retention trigger, system actions, vendors, and backups
Who approved it?	Business owner, Privacy Lead, Security, and Management where required

24. Privacy Incident and Breach Response

Suspected privacy incidents must be reported immediately through the Company’ s incident process. Personnel must not delay reporting while attempting to determine severity or fault.

24.1 Response actions

1. Receive, record, and triage the report; preserve relevant logs and evidence.
2. Contain unauthorized access, sharing, collection, or deletion and protect affected accounts and systems.
3. Identify affected data, people, systems, countries, customers, platforms, and recipients.
4. Assess likelihood and severity of harm, legal and contractual duties, and notification requirements.
5. Notify affected customers, individuals, TikTok Shop, regulators, or authorities where required.
6. Recover, correct records, rotate credentials, delete improper copies, and implement remediation.
7. Complete a documented post-incident review, track corrective actions, and update controls or training.

Notification discipline

Only authorized personnel may make external breach notifications. Notifications must be accurate, timely, coordinated, and consistent with applicable law, contracts, and TikTok Shop requirements.

25. Training, Confidentiality, and Awareness

- Personnel with access to personal data must receive privacy and security training at onboarding and at least annually thereafter.
- Role-specific training must be provided for developers, administrators, support personnel, sales or outreach teams, and staff handling privacy requests or incidents.
- Training must address phishing, secure sharing, data minimization, exports, tokens, sensitive data, incident reporting, and deletion obligations.
- Completion records and confidentiality commitments must be retained as compliance evidence.
- Material policy changes or incidents may trigger targeted refresher training.

26. Monitoring, Audit, Metrics, and Review

The Company will monitor the operation and effectiveness of the privacy program through recurring reviews, evidence checks, metrics, and corrective actions. Reviews are risk-based and scaled to the Company’ s operations.

26.1 Operating cadence

Frequency	Required Activities
Ongoing	Log privacy requests and incidents; review new high-risk changes; remove unnecessary access; complete deletion actions
Monthly	Review overdue privacy requests, deletion exceptions, significant exports, incidents, and remediation status
Quarterly	Sample data inventory accuracy, access, vendor status, retention, and deletion evidence; report material risks
Annually	Full policy review, privacy risk assessment, training, vendor review, retention review, incident exercise, and management approval
Event-driven	Review after a material system, service, legal, platform, vendor, location, or incident change

26.2 Minimum metrics

- Percentage of personnel completing required privacy training.
- Number and status of privacy requests; percentage completed within required timeframes.
- Number of overdue deletion actions and documented exceptions.
- Number, type, severity, and closure status of privacy incidents.
- Percentage of material vendors with current privacy and security review.
- Percentage of material processing activities recorded in the data inventory.
- Number of high-risk changes reviewed before launch and outstanding remediation items.

26.3 Corrective action

Identified deficiencies must be assigned an owner, severity, target date, and remediation plan. Significant or overdue risks must be escalated to Management. The Privacy Lead may recommend suspension of processing that creates an unacceptable or unauthorized privacy risk.

27. Exceptions and Enforcement

27.1 Exceptions

- Exceptions must be documented, time-limited, risk-assessed, approved by the authorized owner, and include compensating controls.
- No exception may authorize conduct prohibited by law, contract, user authorization, or TikTok Shop requirements.
- Exceptions must be reviewed before expiration and closed when no longer required.

27.2 Violations

Violations may result in access removal, corrective training, disciplinary action, contract termination, remediation obligations, notification to affected parties or platforms, and other action appropriate to the severity and applicable requirements.

28. Policy Review, Contact, and Approval

This policy will be reviewed at least annually and after material changes to the Company’ s business, systems, products, processing activities, vendors, laws, platform obligations, or risk environment. Updates must be approved and communicated to relevant personnel.

Legal Entity	江西省深蓝智科文化有限公司
Service Brand	BIGVIRALS
Application	bigvirals-Creator Outreach
Website	https://www.bigvirals.com/
Public Privacy Policy	https://www.bigvirals.com/privacy.html
Privacy and Security Contact	support@bigvirals.com
Approved By	Management of 江西省深蓝智科文化有限公司
Approval Date	July 12, 2026

Management approval statement

Company Management approves this policy as the minimum privacy baseline for daily operations. Business and system owners must implement the controls within their areas and maintain evidence sufficient to demonstrate compliance.

Annex A - Personal Data Classification and Handling Standard

Class	Examples	Minimum Handling
Public	Published website content, public business information, approved marketing materials	May be shared publicly only after authorization; protect integrity and ownership.
Internal	Routine operational procedures, non-sensitive business records, internal contacts	Approved business systems; workforce access based on business need; no public disclosure.
Confidential	Creator and merchant contact data, collaboration records, support cases, account identifiers, contracts, non-public analytics	Role-based access; approved transmission and storage; limit exports; contractual controls for external sharing.
Restricted	Access tokens, client secrets, authentication records, sensitive data, bulk datasets, incident evidence, regulated or platform-restricted data	Strict least privilege; MFA; secure secret storage; enhanced logging; explicit approval; encrypted transfer; no unapproved copies.

Handling decision rules

- When multiple classifications apply, use the highest classification.
- Data classification must consider the risk of aggregation; many low-sensitivity records may form a restricted bulk dataset.
- Tokens, credentials, and private keys are always Restricted.
- Publicly available personal data is still personal data and must be used only for lawful, fair, platform-compliant, and documented purposes.
- De-identified data must be protected against unauthorized re-identification and assessed before external release.

Minimum evidence for handling compliance

Control	Evidence Examples
Collection approval	Privacy review, feature specification, notice, scope approval
Access	Role matrix, access approval, access review, offboarding record
Transfer / sharing	Recipient validation, contract, transfer log, secure link record
Vendor	Due diligence, data-processing terms, sub-processor list, deletion confirmation
Retention / deletion	Retention schedule, deletion ticket, job log, screenshot, provider confirmation
Request handling	Request register, verification record, system-search checklist, response
Incident	Incident ticket, timeline, affected-data assessment, notifications, remediation
Training and review	Attendance records, quiz or acknowledgement, annual review minutes

Annex B - Default Retention and Deletion Schedule

The following periods are default internal targets and must be adjusted when a shorter period is required by purpose, user request, platform instruction, contract, or applicable law, or when a longer period is demonstrably required by law, dispute, security, accounting, or legal hold.

Data Category	Active Retention Trigger / Target	Deletion Treatment
BIGVIRALS account profile	While account is active; review after account closure	Delete or de-identify within 30 days after closure, except necessary legal, billing, fraud, or dispute records
TikTok Shop authorization data and tokens	While authorization and service need remain active	Revoke or invalidate promptly after revocation/disconnection; remove active data within 30 days unless an exception applies
Merchant / seller / creator collaboration records	While the service relationship or active campaign need exists	Delete or de-identify within 30 days after account/service termination unless instructed otherwise or legitimately required
Support tickets and communications	During support relationship and for a reasonable follow-up period	Target 24 months, then delete or de-identify unless needed for dispute, security, or contract evidence
Security, API, and audit logs	Time needed for monitoring, investigation, fraud prevention, and platform requirements	Target 12 months; longer only for active incidents, platform requirements, or documented risk
Billing, invoices, contracts, tax and accounting records	Required business relationship and statutory period	Retain for legally required period; restrict access and delete after expiration
Marketing contact preferences	Until opt-out, invalid contact, or loss of legitimate business need	Suppress from marketing promptly after opt-out; retain minimal suppression record where necessary
Temporary exports and working files	Only while needed for the approved task	Delete promptly after completion; target no more than 30 days
Backups	Normal protected backup cycle	Target expiration or overwrite within 90 days; no routine use after source deletion
Incident records	Through investigation, remediation, legal, contractual, and audit needs	Delete or de-identify after documented closure and applicable retention period

Retention exception record

Required Field	Description
Record / dataset	Specific data affected
Normal deletion date	Date under the approved schedule
Exception reason	Legal hold, dispute, fraud, security, contract, platform instruction, or technical limitation
Authority	Approver and supporting requirement
Restriction	How routine use and access are limited
New review date	Date the exception must be reassessed
Final disposition	Deletion, return, de-identification, or continued lawful retention

Annex C - Privacy Request Operating Procedure

Stage	Owner	Required Action and Evidence
Intake	Privacy Lead / Support	Log request, date, channel, requester, account, scope, and acknowledgement.
Verification	Privacy Lead	Use proportionate identity or authority checks; record method without retaining excessive verification data.
Role determination	Privacy Lead / Business Owner	Determine whether Company acts as controller, processor, or service provider and whether a customer must be involved.
Search and restriction	System Owners	Search relevant systems and vendors; preserve evidence; restrict disputed data where appropriate.
Decision	Privacy Lead / Legal or Management where needed	Apply rights, exceptions, platform obligations, security, fraud, and third-party rights analysis.
Fulfilment	System Owners	Export, correct, delete, restrict, revoke, or otherwise complete approved action.
Response	Privacy Lead / Support	Provide clear response, explanation of exceptions, appeal or complaint route where applicable.
Closure	Privacy Lead	Record systems checked, actions, evidence, date, recipients notified, and outstanding items.

Internal service targets

Activity	Internal Target
Acknowledge request	Within 3 business days
Complete standard request	Within 30 calendar days unless a different legal or contractual timeframe applies
Escalate complex or sensitive request	Within 2 business days of identification
Notify requester of valid extension	Before the original deadline and with the reason
Implement approved deletion / correction	As soon as reasonably practicable after decision

Annex D - Service Provider Privacy Review Checklist

- Business owner, service purpose, contract owner, and termination owner are identified.
- Data categories, subjects, volume, sensitivity, access method, and storage locations are documented.
- Provider acts only on documented instructions and does not sell or independently exploit the data.
- Appropriate confidentiality, security, access, logging, incident, retention, deletion, and audit terms are in place.
- Sub-processors and material locations are disclosed and subject to equivalent obligations.
- Provider can support access, correction, deletion, revocation, export, and evidence requests.
- Provider incident-notification timing and cooperation obligations are suitable for Company and platform requirements.
- Data return and deletion requirements are executable at termination and include backups where appropriate.
- Risk rating, approval, review date, owner, and remediation items are recorded.

Annex E - Collection, Use, Sharing, and Deletion Approval Checklist

Question	Yes / No / N/A	Evidence or Owner
Is the purpose specific, legitimate, necessary, and documented?		
Is each data element necessary, or can less / de-identified data be used?		
Is the source authorized and consistent with platform rules?		
Is an appropriate notice, authorization, consent, contract, or other basis in place?		
Are data subjects, sensitivity, volume, countries, and risks identified?		
Are access roles and privileged actions limited and approved?		
Are storage systems and locations approved and protected?		
Are recipients, vendors, and sub-processors reviewed and contractually controlled?		
Is transfer / sharing limited, secure, and recorded where material?		
Is the retention trigger, period, deletion method, and backup treatment documented?		
Can privacy requests, revocation, correction, and deletion be fulfilled?		
Has the public Privacy Policy or user notice been updated if needed?		
Have Privacy, Security, and Management approvals been obtained where required?		

Annex F - Annual Privacy Program Evidence Checklist

Evidence Item	Minimum Review
Approved policy and revision history	Current, approved, communicated, and reviewed within 12 months
Data inventory / processing records	Material systems and workflows are complete and current
Privacy risk assessments	High-risk and material changes reviewed before launch
Public Privacy Policy	Matches actual processing, legal entity, brand, application, contact, and website
Access and export controls	Sample approvals, access reviews, privileged access, and offboarding evidence
Vendor register and reviews	Current contracts, locations, sub-processors, incidents, deletion and exit plans
Retention and deletion	Schedule, deletion jobs, tickets, exceptions, provider confirmations, backup cycle
Privacy requests	Register, verification, system searches, actions, responses, and timeliness
Incidents	Incident register, severity, notices, remediation, lessons learned
Training	Completion rate, content, acknowledgements, and role-specific refreshers
Metrics and management review	Trends, risks, overdue actions, decisions, and approved remediation

Reference baseline

This policy is designed as a practical internal program and is informed by recognized privacy-risk management and accountability concepts, including the NIST Privacy Framework, widely recognized data-protection principles, and TikTok Shop data security and privacy review expectations. The Company will apply the

requirements that are relevant to its actual services, authorizations, jurisdictions, contracts, and platform obligations.

Implementation evidence note

A strong policy is only one part of compliance. The Company must maintain real evidence that the controls are operating, including data inventories, approvals, access records, vendor reviews, training, request logs, deletion records, incident records, and annual management review.

Annex G - Management Review and Self-Assessment Record

Control Domain	Weight	Self-Assessment Standard
Governance and ownership	10	Approved policy, named owner, management oversight, documented exceptions
Data inventory and purpose	10	Material processing activities recorded, purposes and owners current
Collection and transparency	10	Notices, authorization, minimization, and source controls operating
Storage and access	10	Approved systems, least privilege, MFA, logging, secure handling
Transfer and sharing	10	Recipient validation, minimum data, secure channels, contracts, records
Vendor management	10	Risk reviews, terms, locations, sub-processors, incident and deletion controls
Retention and deletion	15	Schedule, deletion jobs, backup treatment, exceptions, verification evidence
Privacy rights and revocation	10	Request register, verification, timely fulfilment, downstream actions
Incidents and training	10	Prompt reporting, response records, remediation, annual training
Monitoring and review	5	Metrics, sampling, annual review, corrective-action tracking

Annual review sign-off

Review Period	_____
Overall Score	_____ / 100
Material Gaps Identified	_____ _____
Corrective Action Owner	_____
Target Completion Date	_____
Privacy Lead Approval	_____
Management Approval	_____
Approval Date	_____

End of Policy

© 2026 江西省深蓝智科文化有限公司. BIGVIRALS is a product and service brand operated by the Company.