SellerPortal.cz

MARKETPLACES | EXPANSION | BLOG

Amazon SP-API Security Compliance Documentation

How SellerPortal.cz Agency & AI Tools Align with Amazon Data Protection Policy (DPP) Requirements

Prepared by: SellerPortal.cz

Date: 3 June 2026

Classification: Confidential — Amazon SPP Submission

Document Type	SP-API DPP Version	Scope
Security Compliance Statement	Amazon DPP 2024/2025 SP-API Integration Guide	All 10 DPP Security Controls

Executive Summary

SellerPortal.cz is a Czech Amazon FBA consulting agency founded in 2019, specializing in private label expansion across European marketplaces. As a registered Solution Provider applying for access to the Amazon Selling Partner API (SP-API), SellerPortal.cz is committed to full compliance with Amazon's Data Protection Policy (DPP) and Acceptable Use Policy (AUP).

This document formally demonstrates how SellerPortal.cz's operational security practices, internal AI-powered tools, and agency workflows align with all ten security control categories defined in the Amazon SP-API Key Security Control Guidance and Network Protection Guidance documentation.

Compliance Scorecard

Security Control	DPP Section	Status	Priority
Network Protection & Anti-malware	1.1	✓ Compliant	Critical
Access Management	1.2	✓ Compliant	Critical
Credential Management & Password Policy	1.4	✓ Compliant	Critical
Risk Management & Incident Response	1.6	✓ Compliant	Critical
Data Retention Processes	2.1	✓ Compliant	High
Asset Management & PII Controls	2.3	✓ Compliant	High
Encryption at Rest	2.4	✓ Compliant	High
Logging & Monitoring	2.6	✓ Compliant	High
Vulnerability Management	2.7	✓ Compliant	High
Third-party Risk Management	2.8	✓ Compliant	Medium

Key Commitment: SellerPortal.cz designates its founder as the Incident Management Point of Contact (IMPOC) and guarantees notification to security@amazon.com within 24 hours of any detected security incident involving Amazon Information.

1. Company & AI Tools Overview

SellerPortal.cz operates as a boutique Amazon consulting agency with a lean, security-conscious team. Internal operations are supported by proprietary AI-powered tools built on the Anthropic Claude API, which assist with market analysis, profitability calculations, SEO listing generation, and monthly performance reporting for clients.

Tool / System	Purpose	Data Handled	Amazon Info?
Amazon Seller Central	Account management, reporting	Order data, inventory, PII	Yes — Primary
SP-API Integration	Automated data retrieval	Business Reports, Settlement	Yes
Claude AI (Anthropic)	Analysis, report generation	Aggregated/anonymized metrics	No PII
Helium 10 / Jungle Scout	Market research	Public marketplace data	No
Internal Python Scripts	Data processing, PDF/XLSX export	Client performance data	Derived only
Encrypted Password Manager	Credential storage	API keys, login credentials	SP-API keys

2. Security Controls Alignment

The following sections detail SellerPortal.cz's specific implementation of each of the ten security controls mandated by the Amazon Data Protection Policy.

2.1 Network Protection & Anti-malware Controls

DPP Reference: DPP Section 1.1

Amazon DPP Requirement

- Deploy network firewalls and access control lists
- Network segmentation (VLANs, subnets)
- Intrusion detection/prevention systems (IDS/IPS)
- HTTPS/TLS 1.2+ for all data in transit
- Anti-malware updated monthly, cannot be disabled by users
- Endpoint protection on all devices accessing SP-API
- WPA3-encrypted Wi-Fi; guest network isolated via VLAN

SellerPortal.cz Implementation

- ✓ All SP-API communication exclusively via HTTPS/TLS 1.2+
- ✓ Business and guest Wi-Fi separated via VLAN segmentation
- ✓ WPA3 encryption enforced on all office access points
- ✓ VPN required for all remote access to internal systems
- ✓ Up-to-date antivirus deployed on all endpoint devices
- ✓ Firewall rules block unauthorized inbound/outbound traffic
- ✓ Whitelisted IP ranges for SP-API endpoint access
- ✓ Public Wi-Fi prohibited for accessing Amazon Information

2.2 Access Management

DPP Reference: DPP Section 1.2

Amazon DPP Requirement

- Unique identifiers for every user — no shared credentials
- Least-privilege access principle enforced
- Quarterly access reviews for all personnel
- Terminated employee access revoked within 24 hours
- Account lockout after 10 or fewer failed login attempts
- No storage of Amazon Information on personal devices

SellerPortal.cz Implementation

- ✓ Individual accounts per team member — no shared logins
- ✓ Seller Central access granted on need-to-know basis only
- ✓ Quarterly internal review of all active access permissions
- ✓ Immediate access revocation upon end of engagement
- ✓ Account lockout configured at ≤10 failed login attempts
- ✓ Strict prohibition on personal device data storage
- ✓ MFA enforced on all Seller Central and SP-API accounts

2.3 Password & Credential Management

DPP Reference: DPP Section 1.4

Amazon DPP Requirement

- Minimum 12 characters; mixed case, numbers, special chars
- Must not include any part of the user's name
- Password history: last 10 passwords prohibited for reuse
- Max password age: 365 days; min age: 1 day
- MFA via TOTP, hardware token, or biometric
- SP-API credentials encrypted at rest (AES-128 minimum)
- API keys rotated annually with automated processes

SellerPortal.cz Implementation

- ✓ Minimum 12 chars (standard); 16 chars for API/admin accounts
- ✓ Uppercase, lowercase, numbers, and special characters required
- ✓ Last 10 passwords blocked; enforced via password manager
- ✓ Maximum 365-day password lifecycle enforced
- ✓ MFA (TOTP authenticator app) on all Amazon-related accounts
- ✓ All SP-API keys stored in AES-256 encrypted password vault
- ✓ Annual API key rotation with immediate revocation upon breach
- ✓ No credentials stored in source code, spreadsheets, or emails

2.4 Risk Management & Incident Response

DPP Reference: DPP Section 1.6

Amazon DPP Requirement

- Notify Amazon at security@amazon.com within 24 hours
- Incident Response Plan (IRP) reviewed every 6 months
- All 6 phases: Prepare, Identify, Contain, Eradicate, Recover, Learn
- Designated Incident Management Point of Contact (IMPOC)
- Government agency notification per applicable law
- Annual risk assessment reviewed by senior management

SellerPortal.cz Implementation

- ✓ Amazon notified at security@amazon.com within 24 hours
- ✓ GDPR supervisory body notified within 72 hours if PII affected
- ✓ IMPOC designated: Company Founder/Director
- ✓ IRP reviewed bi-annually and after any major incident
- ✓ Documented 5-phase response: Detect → Contain → Assess → Remediate → Review
- ✓ Annual internal risk assessment with documented outcomes
- ✓ All incidents logged in formal incident register with timeline

2.5 Data Retention Processes

DPP Reference: DPP Section 2.1

Data Type	Amazon DPP Limit	SellerPortal.cz Policy	Status
Customer PII (names, addresses)	30 days after order delivery	≤30 days — deleted per delivery	✓
Non-PII order/sales data	18 months maximum	18 months max, then purged	✓
Security & access logs	12 months minimum	12 months minimum retained	✓
SP-API credentials	Encrypted; rotate annually	AES-256 vault; annual rotation	✓
Client reporting data	Per contract + legal obligation	Contractually defined retention	✓

Deletion method: NIST 800-88 compliant secure erasure. PII is never archived beyond the 30-day window unless explicitly required by Czech or EU legal obligations.

2.6 Asset Management & PII Controls

DPP Reference: DPP Section 2.3

Amazon DPP Requirement

- Quarterly inventory of all devices/systems handling PII
- No PII on removable media, personal devices, or public cloud
- Data Loss Prevention (DLP) controls in place
- Baseline security config on all managed assets
- Secure disposal of printed PII materials
- Segregation of duties between change approvers/testers

SellerPortal.cz Implementation

- ✓ Quarterly device inventory maintained and reviewed
- ✓ PII restricted to approved company-managed systems only
- ✓ Removable media and personal devices prohibited for PII
- ✓ No PII stored in unsecured cloud apps (e.g. public Google Drive)
- ✓ All cloud storage encrypted; access controlled and audited
- ✓ Printed documents with PII shredded via cross-cut shredder
- ✓ Change approver and tester roles kept separate for PII systems

2.7 Encryption at Rest

DPP Reference: DPP Section 2.4

Amazon DPP Requirement	SellerPortal.cz Implementation
• AES-128 minimum (AES-256 recommended) for all PII	✓ AES-256 encryption on all devices handling Amazon data
• Encryption applied to drives, servers, databases, backups	✓ Full-disk encryption on all laptops and workstations
• SP-API keys/credentials never stored in plaintext	✓ Database backups encrypted before storage
• Key Management System (KMS) covering full key lifecycle	✓ SP-API credentials stored in AES-256 password vault (KMS)
• Encryption keys rotated at least annually	✓ Encryption key rotation performed annually with audit log
• Compromised keys revoked immediately	✓ Immediate key revocation protocol upon suspected compromise
	✓ SP-API keys never committed to source code repositories

2.8 Logging & Monitoring

DPP Reference: DPP Section 2.6

Amazon DPP Requirement

- Security logs retained for minimum 12 months
- Centralized log collection from all Amazon data systems
- Logs capture: status, timestamps, user IDs, access attempts
- Bi-weekly manual log reviews (or real-time automated)
- Monitor all SP-API access channels and admin dashboards
- Monitor for unauthorized API calls and anomalous patterns

SellerPortal.cz Implementation

✓ Security logs retained ≥12 months in encrypted storage

✓ Centralized logging from all systems accessing Amazon data

✓ All API calls logged with timestamp, user, and outcome

✓ Bi-weekly log review conducted by designated IMPOC

✓ Automated alerts configured for unusual API request patterns

✓ Seller Central login activity monitored for anomalies

✓ Failed authentication attempts trigger immediate alert

2.9 Vulnerability Management

DPP Reference: DPP Section 2.7

Amazon DPP Requirement

- Vulnerability scans every 30 days on all systems
- Annual penetration testing by qualified professionals
- Critical vulnerabilities remediated within 7 days
- High-risk vulnerabilities remediated within 30 days
- Geographically separated backup sites with RTO/RPO
- Code scanned before each software release

SellerPortal.cz Implementation

✓ Monthly vulnerability scans on all internet-facing systems

✓ Annual penetration test by qualified third-party firm

✓ Critical CVEs patched within 7 days — zero exceptions

✓ High-risk findings resolved within 30-day SLA

✓ Backup and recovery procedures tested quarterly

✓ All internal scripts security-reviewed before deployment

✓ OS and application patches applied on monthly cadence

2.10 Third-party Risk Management

DPP Reference: DPP Section 2.8

Amazon DPP Requirement	SellerPortal.cz Implementation
• Annual risk assessment of all vendors/subcontractors • Vendors assessed before granting access to Amazon data • Security standards contractually required of subcontractors	✓ Annual security review of all third-party tools and APIs ✓ Anthropic Claude API: data processed per Anthropic's DPA — no PII transmitted ✓ Helium 10 / Jungle Scout: public market data only — no Amazon PII shared ✓ Vendor DPA agreements in place for all data processors ✓ No Amazon PII shared with third-party tools without explicit authorization

3. Operational Compliance Schedule

SellerPortal.cz commits to the following ongoing operational security tasks at the cadences mandated by the Amazon Data Protection Policy.

Required Task	Amazon DPP Cadence	SellerPortal.cz Implementation	Owner
Conduct log reviews	Bi-weekly	Bi-weekly manual review by IMPOC	IMPOC/Founder
Update anti-malware tools	Monthly	Automated monthly antivirus definition updates	IT / Founder
Vulnerability scans on all systems	Monthly	Monthly automated + manual scan	IMPOC
Review all personnel & service access	Quarterly	Quarterly access audit; remove dormant accounts	Founder
Inventory of devices handling PII	Quarterly	Quarterly asset inventory review	Founder
Test backup & recovery procedures	Quarterly	Quarterly restore test with documented result	IT / Founder
Rotate Amazon API keys	Annually	Annual rotation with audit log entry	Founder
Rotate encryption keys	Annually	Annual KMS rotation; immediate if compromised	Founder
Security awareness training	Annually	Annual DPP & IT security training for all users	All Staff
Penetration testing	Annually	Annual test by qualified third-party firm	Third Party
Formal third-party security assessments	Annually	Annual vendor risk assessment review	Founder

4. Critical Response Timelines

The following critical response timelines are mandated by the Amazon DPP and are formally adopted into SellerPortal.cz's Incident Response Plan.

Response Requirement	Amazon DPP Timeline	SellerPortal.cz Commitment
Notify Amazon (security@amazon.com) of any security incident	**24 hours**	✓ **Within 24 hours — IMPOC on-call**
Revoke access for terminated employees	**24 hours**	✓ **Immediate upon termination**
Remediate critical-risk vulnerabilities	**7 days**	✓ **7-day patch SLA enforced**
Remediate high-risk vulnerabilities	**30 days**	✓ **30-day patch SLA enforced**
Delete PII after order delivery	**30 days**	✓ **Automated 30-day deletion policy**
Notify GDPR supervisory body (if PII breach)	**72 hours**	✓ **Czech DPA notified per GDPR Art. 33**

5. Formal Declaration

SellerPortal.cz hereby formally declares that the security controls, policies, and procedures described in this document are actively implemented and maintained within our organization. We commit to full compliance with the Amazon Data Protection Policy (DPP) and Acceptable Use Policy (AUP) as a condition of SP-API access.

We acknowledge our obligation to notify Amazon at **security@amazon.com** within **24 hours** of any security incident involving Amazon Information, and to cooperate fully with any Data Security Assessment conducted by Amazon.

This document is reviewed and updated on a bi-annual basis and following any material change to our systems, personnel, or security posture.

Authorized Signatory	Organization	Date	Role
SellerPortal.cz	SellerPortal.cz s.r.o.	3 June 2026	Founder & IMPOC
_____	IČO: [company registration]		