GLOBAL PRIVACY POLICY

Last Updated: 2026-03-09

Version 1.0

This Global Privacy Policy describes how Blueshift Cybersecurity, Inc. (“Blueshift,” “we,” “us,” or “our”) may collect, use, disclose, and otherwise process personal information in connection with certain of our business operations, including our Websites, software products, partner-channel activities, and managed security services, and should be read together with any more specific privacy notice, cookie disclosure, or customer-facing data protection document that applies to the relevant interaction, product, service, or jurisdiction, including any supplemental disclosures required under the laws of the European Economic Area (“EEA”), Switzerland, and the United Kingdom (“UK”). In the event of any inconsistency between this Global Privacy Policy and a more specific privacy notice, cookie disclosure, customer-facing data protection document, or an applicable written customer agreement that expressly governs the relevant processing activity, the more specific document or agreement will control to the extent of that inconsistency. This Global Privacy Policy is generally informational and does not by itself create contractual obligations except to the extent expressly incorporated into an applicable written agreement.

This Global Privacy Policy applies to personal information we collect when:

• You visit or interact with our Websites, including www.blueshiftcyber.com and any other Blueshift websites or online services that link to this Global Privacy Policy (“Websites”); • You communicate with us, including through sales, marketing, support, events, or channel and partner activities; • You use our Software Services, including the IntelliThreat AI Platform (“Software Services”); and • You receive our managed security services, including Security Operations Center (“SOC”) and Managed Extended Detection & Response (“XDR”) services (“Managed Services”).

This Global Privacy Policy does not apply to job applicants, candidates, or employment-related personal information, which may be governed by separate privacy disclosures where applicable.

1. ROLES AND RESPONSIBILITIES

Blueshift’s role with respect to personal information depends on the context in which the information is processed.

Software Services (IntelliThreat AI Platform) When we process personal information on behalf of a customer in connection with the IntelliThreat AI Platform, whether the Software Services are purchased directly from Blueshift or through an authorized reseller, distributor, or other channel partner, Blueshift generally acts as a data processor, service provider, contractor, or similar role under applicable privacy laws solely to the extent of such processing. Our processing of such data is governed by the applicable Platform Master Subscription Agreement, applicable Order, and Data Processing Addendum — IntelliThreat AI Platform, solely as and to the extent incorporated thereunder.

Managed Services (SOC and XDR) When we provide Managed Services, whether directly or in coordination with an authorized reseller, distributor, or other channel partner, Blueshift's role with respect to personal information depends on the nature of the Managed Services, the specific processing at issue, and the applicable contract stack, and Blueshift may act as a data processor, service provider, contractor, data controller, business, or similar role under applicable privacy laws, as described in the applicable managed services agreement, statement of work, services addendum, any applicable data processing terms, and related customer documentation. For clarity, this Global Privacy Policy does not expand Blueshift's processing obligations or service commitments for Managed Services beyond those expressly set forth in the applicable written agreement and related customer-facing documentation governing the relevant Managed Services.

Website, Marketing, and Business Operations When you interact with our Websites, marketing activities, partner and channel programs, or business operations, Blueshift generally acts as a data controller with respect to personal information collected in those contexts, except to the extent a different role is expressly described in an applicable supplemental notice, customer-facing document, or written agreement.

2. PERSONAL INFORMATION WE COLLECT

We may collect the following categories of personal information, depending on your interaction with us:

Business Contact Information. Name, job title, company name, business email address, business phone number, and mailing address.

Account and Relationship Information. Information related to your organization's relationship with Blueshift, including account identifiers, subscription details, support interactions, communications, and information relating to customer, reseller, distributor, referral, and integration partner relationships.

Website and Usage Information. Information such as IP address, browser type, device information, pages visited, referring URLs, and interaction data that may be collected when you use our Websites, including through cookies and similar technologies.

Communications Information. Information you provide when you contact us, submit forms, request demos, attend events, participate in partner or channel discussions, or communicate with our sales or support teams.

Customer Data. Data processed in connection with the IntelliThreat AI Platform or Managed Services may include security telemetry, logs, identifiers, metadata, support content, and related operational information. Customer Data is processed in accordance with customer instructions, applicable agreements, incorporated addenda, and, where relevant, applicable law and documented operational requirements reasonably necessary to provide, secure, maintain, support, and administer the applicable products or services. Blueshift's role with respect to such Customer Data depends on the applicable product line, service context, and governing agreement or privacy disclosure applicable to that processing.

We do not generally seek to collect sensitive personal information such as government identifiers, biometric data, or health information. However, depending on your interaction with

us and the context in which our Websites, products, or services are used, certain telemetry, log, device, platform, account, communication, or support-related data that we or our service providers process may incidentally include data elements that could be treated as sensitive personal information under applicable law.

3. HOW WE USE PERSONAL INFORMATION

We use personal information for the following purposes:

• To operate, maintain, and improve our Websites, Software Services, and Managed Services; • To establish and manage customer, reseller, distributor, referral, integration, and other partner relationships; • To provide customer and partner support and respond to inquiries; • To communicate about products, services, updates, security notices, and, where permitted by law, promotional materials, and to honor applicable requests to opt out or unsubscribe from marketing communications, provided that we may still send service-related, transactional, security, legal, or other non-marketing communications where permitted by law; • To conduct sales, marketing, channel, and business development activities; • To analyze usage trends and improve functionality and performance; • To comply with legal obligations and enforce our agreements; and • To protect the security, integrity, and availability of our systems and services.

We process personal information only where we have a valid legal basis, including, as applicable, where processing is necessary for the performance of a contract with you or your organization, to take steps at your request before entering into a contract, for our legitimate interests (such as operating, securing, improving, and promoting our business, products, and services, except where those interests are overridden by your data protection rights), to comply with legal obligations, or based on your consent where required by law. In limited circumstances, we also may process personal information where necessary to establish, exercise, or defend legal claims or as otherwise permitted by applicable law.

4. HOW WE SHARE PERSONAL INFORMATION

We may share personal information with:

Service Providers and Subprocessors. Thirdparty vendors may provide services on our behalf in connection with our Websites, Software Services, Managed Services, or business operations, such as cloud hosting, customer support, email delivery, analytics, security monitoring, and related operations. Where Blueshift processes personal information on behalf of a customer, applicable vendors engaged for that processing may act as subprocessors under the relevant customer agreement, the Data Processing Addendum — IntelliThreat AI Platform, any applicable Managed SOC & XDR Services Addendum, any applicable managed-services-specific data processing terms, or related documentation, in each case solely to the extent applicable to the relevant processing activity. Where appropriate, these providers are subject to contractual or other obligations to protect personal information and use it only for authorized purposes.

Affiliates. Blueshift affiliates and subsidiaries for internal business operations consistent with this Global Privacy Policy.

Business Partners. Authorized resellers, distributors, referral partners, integration partners, channel partners, and other business partners where reasonably necessary to support customer

and partner relationships, evaluate opportunities, provide joint offerings, facilitate direct or indirect sales motions, or conduct related business operations, in each case subject to applicable law and any applicable contractual restrictions.

Legal and Regulatory Authorities. Where required to comply with applicable law, legal process, or governmental requests, or to protect the rights, safety, and security of Blueshift, our customers, or others.

Corporate Transactions. In connection with a merger, acquisition, financing, reorganization, or sale of assets, subject to appropriate confidentiality protections.

Blueshift does not sell or share personal information as those terms are defined under applicable law, except to the extent a particular disclosure or use of cookies or similar technologies on our Websites or online services is deemed a "sale" or "sharing" under applicable law, as further described in our California Privacy Notice, Cookie Policy, or other applicable privacy notice, and Blueshift does not sell personal information for money or for consideration in the traditional sense.

5. COOKIES AND TRACKING TECHNOLOGIES

We use cookies and similar technologies on our Websites to help operate and secure the Websites, remember preferences, analyze usage, and support marketing and campaign measurement activities. You can manage cookie preferences through your browser settings and, where required by law or made available on the relevant Website, our cookie banner or preference center. Our Websites do not currently respond to browser "Do Not Track" signals in all cases, but we may recognize Global Privacy Control or similar browser-based preference signals where required by applicable law and where technically supported, configured, and recognized in connection with the relevant Website, browser, device, or processing activity. Additional details are available in our Cookie Policy, which should be read together with this Global Privacy Policy as updated from time to time. For clarity, the Cookie Policy addresses cookies and similar technologies used on our Websites and online services and does not by itself alter how Customer Data is processed in connection with the IntelliThreat AI Platform or Managed Services under applicable customer agreements unless expressly incorporated therein.

6. DATA RETENTION

We retain personal information for as long as reasonably necessary for the purposes described in this Global Privacy Policy, including to comply with legal obligations, resolve disputes, protect our interests, and enforce agreements. The retention period applicable to particular personal information depends on the nature of the information, the context in which it was collected, the purpose for which it is used, applicable contractual requirements, legal, regulatory, accounting, and reporting obligations, applicable limitation periods, and whether retention is reasonably necessary for security, incident response, fraud prevention, backup, archiving, business continuity, or the establishment, exercise, or defense of legal claims. In general, and unless a longer period is required or permitted by applicable law or contract, we retain Business Contact Information, Account and Relationship Information, and Communications Information for the duration of the relevant relationship and for a reasonable period thereafter to support follow-up

communications, recordkeeping, contract administration, compliance, dispute resolution, and the establishment, exercise, or defense of legal claims; Website and Usage Information for as long as reasonably necessary for the operational, security, analytics, and marketing purposes described in this Global Privacy Policy and our Cookie Policy, after which it is deleted, aggregated, deidentified, or otherwise retained only as permitted by applicable law; and Customer Data only for the period determined by the applicable customer agreement, documented customer instructions, product configuration, service scope, and legal or operational requirements applicable to the relevant processing context.

Customer Data processed through the IntelliThreat AI Platform is retained in accordance with the applicable Data Processing Addendum, relevant customer configurations, applicable Orders, documented customer instructions, and applicable legal or operational requirements. Customer Data processed in connection with Managed Services is retained in accordance with the applicable Managed SOC & XDR Services Addendum, any applicable Data Processing Addendum or managed-services-specific data protection terms, documented customer instructions where applicable, and applicable legal or operational requirements. Where required or appropriate, we may also retain limited information relating to Customer Data for backup, archiving, audit, security, fraud prevention, billing, legal compliance, or the establishment, exercise, or defense of legal claims, in each case subject to applicable contractual and legal restrictions.

7. DATA SECURITY

We implement commercially reasonable administrative, technical, organizational, and physical measures designed to protect personal information against unauthorized access, disclosure, alteration, or destruction. No security measures are infallible, and we cannot guarantee absolute security.

8. INTERNATIONAL DATA TRANSFERS

Blueshift is based in the United States, and personal information may be processed in the United States or other locations where we or our service providers operate. Where required by law, we implement appropriate safeguards for international data transfers, such as adequacy decisions, the European Commission's Standard Contractual Clauses, the UK International Data Transfer Addendum or other UK-approved transfer mechanisms, contractual protections, and, where appropriate, supplementary technical, organizational, or administrative measures, as applicable to the relevant processing context. You may contact us using the details below to request additional information about applicable transfer safeguards, where required by law.

9. YOUR PRIVACY RIGHTS

Depending on your location, applicable law, and the nature of our relationship with you, you may have certain rights to access, correct, delete, or restrict the processing of your personal information, or to object to certain processing activities, subject to applicable exceptions and limitations. If you are located in the EEA, Switzerland, or the UK, and to the extent applicable law applies, you also may have the right to request data portability, to object to processing based on legitimate interests, to withdraw consent at any time where processing is based on consent

(without affecting the lawfulness of processing based on consent before its withdrawal), to opt out of or unsubscribe from direct marketing communications, and to lodge a complaint with your local supervisory authority or data protection regulator. Requests may be submitted to privacy@blueshiftcyber.com or dsr@blueshiftcyber.com. We may need to verify your identity and authority before responding, and we may decline or limit a request where permitted by applicable law. Where Blueshift processes personal information solely on behalf of a customer as a processor, service provider, contractor, or similar role under the applicable customer agreement, we may direct your request to the relevant customer or advise you to contact that customer directly.

For purposes of the GDPR and the UK GDPR, Blueshift has not appointed an EU representative or a UK representative under Article 27 of the GDPR or the UK GDPR because Blueshift currently assesses, based on its then-current relevant processing activities, that such appointment is not required or that an applicable exemption is available, including where processing is occasional, does not include large-scale processing of special categories of personal data or personal data relating to criminal convictions and offences, and is unlikely to result in a risk to the rights and freedoms of individuals. If that position changes, we will update this Global Privacy Policy and provide the relevant representative contact details.

California residents should refer to our California Privacy Notice, which supplements this Global Privacy Policy, for additional information about rights under California law.

10. CHILDREN'S INFORMATION

Our products and services are not intended for use by children, and we do not knowingly seek to collect personal information from children.

11. CHANGES TO THIS PRIVACY POLICY

We may update this Global Privacy Policy from time to time to reflect changes in our practices, services, privacy-document set, or applicable law. We will post the revised version on our Websites and may provide additional notice of material changes where required by applicable law. To the extent permitted by law, your continued interaction with the applicable Websites, products, or services after any update becomes effective signifies your acknowledgment of the revised policy, but does not by itself create contractual obligations except to the extent this Global Privacy Policy is expressly incorporated into an applicable written agreement.

12. CONTACT US

If you have questions about this Global Privacy Policy or our privacy practices, please contact:

Blueshift Cybersecurity, Inc.
Email: privacy@blueshiftcyber.com
2022 Hendry Street
Fort Myers, Florida 33901