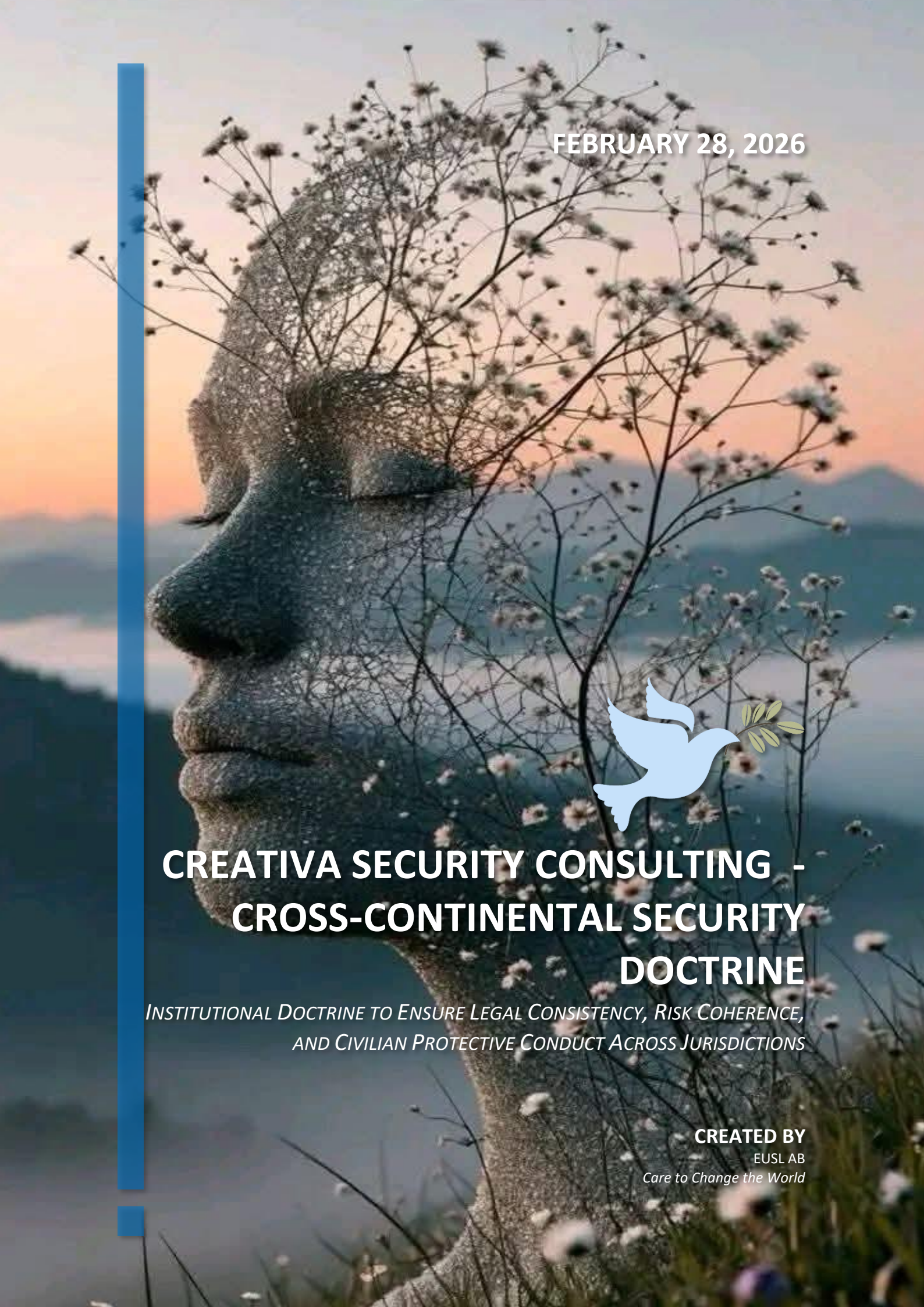

FEBRUARY 28, 2026

CREATIVA SECURITY CONSULTING - CROSS-CONTINENTAL SECURITY DOCTRINE

INSTITUTIONAL DOCTRINE TO ENSURE LEGAL CONSISTENCY, RISK COHERENCE, AND CIVILIAN PROTECTIVE CONDUCT ACROSS JURISDICTIONS

CREATED BY
EUSL AB
Care to Change the World

Table of Contents

CROSS-CONTINENTAL SECURITY DOCTRINE

INTRODUCTION

This Doctrine establishes the common protective logic governing Creativa Center Universe (CCU) operations across Europe, Africa, and other regions. Its purpose is to ensure that security decisions are made within a unified legal and ethical framework, producing predictable outcomes across dissimilar legal regimes and risk profiles. It consolidates the principles already articulated in the Business Plan and in the Mandate Documents and translates them into a jurisdiction-sensitive, yet globally coherent, operating doctrine.

Within the European Union, security and safeguarding activities must be conducted under the constraints of the General Data Protection Regulation (GDPR) and the Swedish Camera Surveillance Act (for Sweden), including documented necessity, proportionality, accountability, and supervision by competent authorities. The removal of prior permit requirements in Sweden for many public-access surveillance scenarios does not reduce obligations to document legitimate interest; if anything, it elevates the importance of internal governance and ex post accountability.

The Doctrine is civilian and non-militarised by design. It requires that armed protective elements in foreign jurisdictions, when necessary and lawful, be performed by licensed local providers or state units, with Creativa retaining strategic planning and oversight only. It integrates national threat perspectives and supervisory expectations, including those periodically published by the Swedish Security Service, which frame hybrid threats, terrorism risk, and infrastructure vulnerabilities affecting the Swedish and broader European operating context.

CHAPTER 1 — THREAT AND RISK LANDSCAPE OVERVIEW

The threat and risk landscape is differentiated across four principal operating categories: European Union civilian environments; COMESA and EAC/SADC environments with varying governance and infrastructure maturity; fragile or semi-fragile environments; and special contexts such as ports, airports, and logistics corridors supporting ECHO modules.

European Union environments are characterised by strong rule-of-law, data-protection primacy, and public-order policing led by state authorities. Even when crime or public disorder risk is elevated, the default operational posture remains unarmed private security with rapid escalation to police, strict surveillance constraints, and documented impact assessments underpinning camera use and monitoring.

COMESA and EAC/SADC contexts present heterogeneous risks: opportunistic and organised crime, cargo theft, corruption exposure, and episodic political volatility that can affect road movement, ports, and border processes. While legal frameworks vary by country, the lawful approach for foreign civilian organisations generally involves contracting licensed local armed escorts where required, with the international principal maintaining itinerary control, communications discipline, and crisis thresholds. This model mirrors the widely adopted posture of civilian international actors and is aligned with a governance-first approach that preserves political neutrality. (General practice orientation anchored in EU legal posture and Swedish supervisory expectations for civilian conduct.)

Fragile or semi-fragile environments require heightened attention to route security, safe-haven mapping, curfew observance, and rapid escalation protocols, acknowledging that the presence of international assets and perceived financial capacity increases targeting risk. EU-derived data-protection and accountability norms remain relevant to the extent that personal data are processed by CCU entities or their processors, even when operations are physically outside the EU, subject to local law and international transfer rules.

Across all categories, surveillance and information handling must respect legality, necessity, proportionality, and limited retention, with IMY's guidance emphasising documentation and reassessment, particularly after the 2025 changes in Sweden's Camera Surveillance Act and the Authority's stated intent to increase ex post supervision.

CHAPTER 2 — PRINCIPLES OF PROTECTIVE SECURITY ACROSS REGIONS

The following principles govern all protective activity and apply uniformly, with local adaptations solely for legal compliance and risk reality.

First, legality and proportionality. Protective measures must have a clear legal basis, be necessary to achieve a legitimate security purpose, and be proportionate to the risk presented. In the EU, this includes GDPR compliance for any personal data processing, with lawful bases, purpose limitation, data minimisation, retention control, records of processing, and, where appropriate, data-protection impact assessments.

Second, civilian posture and escalation discipline. Private security remains civilian in character. Use of force is restricted to lawful self-defence and immediate necessity; all other coercive powers are reserved to state authorities. In Sweden and most EU contexts, armed private security is tightly constrained or disallowed; the operational norm is unarmed presence with a documented escalation pathway to public authorities. Surveillance implementations are subject to the Camera Surveillance Act's complements to GDPR, with ongoing accountability even after the 2025 permit changes.

Third, local capability utilisation. In non-EU jurisdictions where risk and law so permit, armed functions are outsourced to licensed local security providers or state units under written terms that define scope, conduct, reporting, and termination rights. The principal retains strategic control of routing, timing, communications, and crisis criteria while preserving political neutrality and host-country legal compliance. (Civilian posture and neutrality principles grounded in Swedish and EU supervisory perspectives on security and national-security context.)

Fourth, information governance and transparency. All monitoring, access-control logging, journey data, and incident documentation must meet GDPR principles when CCU is a controller or processor, with special care in youth environments and mixed communities. Documentation of legitimate-interest balancing is mandatory for camera surveillance in Sweden and recommended as good practice elsewhere to evidence accountability and proportionality.

Fifth, workforce safety and competence. Systematic risk assessment, training, and incident aftercare are essential to meet employer duties under Swedish work-environment law for Sweden-based staff and to meet equivalent obligations where applicable abroad, recognising that the duty to provide a safe system of work follows the employer and not merely the jurisdiction.

These principles produce a unified standard: legally anchored, civilian, auditable, and ethically robust across borders.

CHAPTER 3 — EUROPE DOCTRINE

The Europe Doctrine operationalises the above principles for EU environments, with Sweden as the primary reference jurisdiction for licensing, surveillance, and workforce duties. It is designed for EUOS properties, travel within the Schengen area, and EU-based logistics supporting ECHO.

Security presence is safeguarding-compatible. Guarding, reception control, and patrols in EUOS and comparable sites must be conducted with a de-escalatory posture and sensitivity to youth and mixed communities. Surveillance and access control must be underpinned by GDPR-compliant governance (lawful basis; data minimisation; retention limits; role-based access; secure storage) and, where camera surveillance is deployed, the obligations of the Camera Surveillance Act, including signage, scoping, and periodic reassessment. In Sweden, since 1 April 2025, no prior permit is required in many scenarios, but a documented legitimate-interest assessment is mandatory and subject to IMY's supervisory review.

Unarmed protection norms apply as default. Movements of principals and staff in the EU are conducted unarmed, with risk-based routing, timing controls, discreet protective accompaniment, and, where justified, the use of armoured vehicles as a defensive measure without altering the civilian character of the activity. The lawful escalation path is to the police and emergency services; private security does not assume public powers. Swedish national-security posture publications underscore hybrid threat awareness, infrastructure vigilance, and the importance of coordinated protection with public authorities — considerations that inform route selection, event planning, and information security in EU member states.

Monitoring integrity and record-keeping are mandatory. Command functions must maintain incident logs, response rationales, and surveillance access records. GDPR requires records of processing and, for higher-risk surveillance, DPIAs; the Camera Surveillance Act complements these duties in Sweden, and IMY's public guidance stresses accountability, proportionality, and post-change reassessment.

Workforce protection is continuous. Employers must ensure risk assessment, training, and after-incident support for personnel assigned to guarding and monitoring roles, including night work and crowd-facing contexts. The Swedish Work Environment Act outlines the preventive and systematic nature of employer duties, which the Company treats as a baseline standard for EU operations.

Finally, **political neutrality and reputational prudence** bind all activities. In EU civilian environments, where rule-of-law and data-protection regimes are sophisticated and public trust is central, security actions must be visibly lawful, restrained, and respectful of fundamental rights, aligning with GDPR's framing of data protection as a fundamental right and with national supervisory expectations for proportional surveillance.

CHAPTER 4 — AFRICA DOCTRINE

The Africa Doctrine governs Creativa operations in COMESA, EAC/SADC, and other African jurisdictions by combining civilian protective practice with strict host-country legal compliance and partnership with licensed local providers for any armed components. The Company, as a European civilian security enterprise, does not deploy armed personnel abroad; where armed protection is lawful, necessary, and proportionate, it is procured through vetted local firms or provided by state authorities under written terms that define scope, conduct standards, reporting, and termination rights. This preserves legality, neutrality, and accountability while ensuring that itinerary control, route selection, communications integrity, and emergency thresholds remain under Creativa's strategic direction. This posture mirrors

the lawful civilian approach expected of EU-based entities, and is consistent with Swedish supervisory expectations around civilian/non-militarised security roles.

Movements, convoys, and logistics supporting ECHO equipment observe a layered protection model. The Unit prescribes custody documentation, tamper-evident controls, storage standards, and convoy discipline; licensed local escorts are contracted where host law permits, while Creativa maintains communications and escalation control. Camera or access-control technologies deployed around temporary depots or permanent sites must comply with local law; where Creativa or its EU processors handle personal data, GDPR duties concerning lawfulness, minimisation, retention, and accountability remain engaged to the extent of EU territorial scope and controller responsibilities. In practice, this requires documented purposes, role-based access, and retention limits, with special protections if any data of minors is processed in training or community contexts linked to EUOS replication.

Airport/port interfaces require early liaison with competent authorities, pre-clearance of security arrangements, and custody-chain documentation from offload to inland transport. Deviations, interference, or attempted redirection trigger immediate escalation to public authorities and a halt pending clarification. Where site monitoring is envisaged, proportional deployment and local-law compliance are mandatory; Swedish practice after the 2025 Camera Surveillance Act update—emphasising documented legitimate interest, proportionality, and reassessment—serves as an internal benchmark for accountability even when operating under different local statutes.

Political interface is restrained, neutral, and documented. Engagements with police or military units are limited to operational coordination, with no assumption of state functions. All personnel are briefed on local law, corruption-avoidance protocols, and rules for interaction with public officials. Intelligence handling remains within lawful corporate-security bounds; intrusive methods and any activity resembling intelligence-service tradecraft are prohibited. Swedish national-security publications, which highlight hybrid threats and infrastructure vulnerabilities, inform pre-deployment risk mapping and communications discipline for Swedish-linked teams, even when outside the EU.

Medical contingencies, evacuation thresholds, and safe-haven triage are pre-authorised in movement plans. Documentation of incidents and near-misses is contemporaneous and limited to necessary facts, reflecting GDPR accountability standards whenever Creativa is a controller or processor of personal data generated by these operations.

CHAPTER 5 — SPECIAL SITUATIONS DOCTRINE

Special situations—natural disasters, political instability, kinetic unrest, high-risk travel, and rapid evacuation—require pre-agreed thresholds and executable contingencies across jurisdictions. Activation is triggered by objective indicators: government advisories, airport and port closures, curfews, credible threat reporting, or immediate proximity incidents. In EU contexts, activation protocols must also consider data-protection constraints on monitoring and tracking personnel; risk communications and location processing must have a lawful basis and observe minimisation and retention limits.

Natural disasters call for life-safety primacy: shelter-in-place or evacuation per pre-mapped routes, verified fuel and logistics nodes, and redundant communications. Surveillance or access-control adjustments introduced during a disaster—expanded camera coverage, emergency logging, ad hoc visitor vetting—must be documented with purpose, necessity, and duration, and reversed once the emergency subsides. In Sweden, IMY's post-April 2025 accountability stance underscores the

importance of recorded legitimate-interest assessments and reassessment when surveillance scope changes, a practice Creativa internalises for crisis-period deployments and roll-backs.

Political instability or civil unrest triggers movement reductions, low-profile routing, convoy consolidation with licensed local escorts where lawful, and a heightened threshold for pausing operations. Neutrality is maintained at all times; escalatory or symbolic posturing is strictly prohibited. Swedish security-service reporting on hybrid threats and ideological polarisation serves as a strategic reminder to limit overt patterns that can draw attention to Swedish-linked entities, and to moderate information exposure on itineraries and assets.

High-risk travel for executives or technical teams is authorised only with written risk assessments, safe-haven mapping, contingency routing, and medical/MEDEVAC links. Data generated by tracking or monitoring of staff during such missions is processed under GDPR principles when Creativa acts as controller/processor, with retention restricted to the operational window and immediate post-mission review; where camera surveillance supports staging areas in Sweden, the Camera Surveillance Act complements GDPR obligations and requires transparency and proportional scoping.

Evacuation scenarios are codified as a last resort: clear abort criteria, rally points, layered comms (primary, secondary, tertiary), contracts with vetted local transporters, and prompt notification to public authorities. Post-event, documentation is reviewed under GDPR's accountability principle and, in Sweden, under IMY's ex post oversight posture for any extraordinary surveillance measures adopted during the incident.

CHAPTER 6 — COMMAND, CONTROL, AND COMMUNICATION

Command and control are centralised to preserve legality, audibility, and proportionality across borders. A Swedish-based command function maintains operational awareness, documents decisions, and integrates incident intake, escalation, and reporting. In Sweden and the EU, information flows that involve personal data—location, video, access logs—are controlled under GDPR: defined purposes, role-based access, retention schedules, and security of processing. Where camera surveillance is used in Sweden, documentation of legitimate interest and periodic reassessment is required in line with the Camera Surveillance Act's framework and IMY guidance following the 1 April 2025 changes.

Decision rights are pre-delegated and documented: routine site incidents are handled locally under licensed guarding SOPs; cross-border movements and any request for armed escorts abroad require command-level approval and written legal validation. Replacement of the operational manager in Sweden, or any change to the authorised scope of licensed activities, triggers immediate notifications to the County Administrative Board, consistent with Swedish authorisation and supervision practice. These statutory links ensure that operational command does not drift outside the bounds set by *Lag (1974:191) om bevakningsföretag*.

Communications employ encrypted channels with redundancy and immutable audit trails for critical directives. Changes to surveillance coverage, escalation thresholds, or brigade composition in response to dynamic threats are logged, time-stamped, and subject to post-operation review. Where EU data are processed, GDPR imposes records-of-processing and security-of-processing duties; where the Company operates in Sweden, IMY's accountability expectations require that such adjustments be demonstrably necessary and proportionate, with reassessment upon material change.

Liaison with public authorities is disciplined and respectful of sovereignty. In Sweden and the EU, the default escalation is to the police and emergency services; in African jurisdictions, liaison is coordinated

with the relevant ministry, police, or port/airport security according to local legal hierarchy. The Swedish Security Service's emphasis on hybrid threats and infrastructure vigilance reinforces the Company's requirement to maintain situational context and to avoid information practices that increase exposure or signal high value.

In sum, the command, control, and communication architecture is designed to be lawful, civilian, and reviewable: Swedish licensing anchors the Company's authority, GDPR and the Camera Surveillance Act frame information and surveillance conduct, and host-country law governs any armed provision through licensed local actors. This produces traceable, proportional, and coherent protective conduct across all operating regions.

References

- *Lag (1974:191) om bevakningsföretag* (authorisation; supervision; personnel approvals): Riksdagen; County Administrative Boards guidance (authorisation, personnel approvals, annual reporting, change of operational manager): Länsstyrelsen Stockholm.
- GDPR — Regulation (EU) 2016/679 (lawfulness, minimisation, accountability, DPIA, records of processing): EUR-Lex.
- Camera Surveillance Act (*Kamerabevakningslag (2018:1200)*) and 2025 accountability practice: Riksdagen; IMY camera-surveillance guidance (post-permit removal; LIA/accountability; reassessment): IMY; policy update summary and guidance context: Digital Policy Alert.
- Swedish Security Service strategic context (hybrid threats, infrastructure vigilance): Säkerhetspolisen annual report 2024–2025 (EN).