TOOL KIT

From Boots on the Ground to Bytes in Cyberspace

A Comprehensive Guide for Responsible Technology Use by the Private Security Sector

Anne-Marie Buzatu

Version 1.1
Geneva, June 2026

ICT for peace foundation

ICoCA The Responsible Security Association

INTRO
From Boots on the Ground to Bytes in Cyberspace

A Comprehensive Guide for Responsible Technology Use by the Private Security Sector

Anne-Marie Buzatu · Version 1.1, June 2026 · ICT4Peace Foundation / ICoCA

Version 1.1 — Key Updates

- **EU AI Act**: Prohibited practices enforceable from February 2025; Annex III high-risk obligations mandatory from December 2027 (provisional — postponed by EU Digital Omnibus, May 2026)
- **CSDDD**: Mandatory HRDD for large companies; phased from 2027; director-level accountability
- **Pall Mall Process**: Code of Practice endorsed by 25 states, April 2025 — primary standard for commercial cyber intrusion tools
- **NIST PQC Standards**: FIPS 203/204/205 published August 2024; HNDL makes migration a present obligation
- **EU Platform Work Directive**: First EU law on algorithmic management — in force December 2024
- **EU Data Act**: IoT data access rights and cloud-switching rights in force September 2025
- **NIS2 Directive**: Mandatory 24h/72h incident notification; MSPs/MSSPs explicitly covered — transposed October 2024
- **ISO/IEC 27001:2022**: 2013 edition now obsolete — transition deadline October 2025 passed
- **NIST CSF 2.0**: Adds Govern function; expanded scope — published February 2024
- **boots2bytes.ch**: Toolkit now available online at boots2bytes.ch

Overview

This toolkit — From Boots on the Ground to Bytes in Cyberspace — is a practical, human rights-aware resource for private security companies (PSCs) navigating the responsible use of information and communications technologies (ICTs). It was developed by the ICT4Peace Foundation in collaboration with ICoCA and draws on the UN Guiding Principles on Business and Human Rights, the International Code of Conduct for Private Security Service Providers (ICoC), and a comprehensive review of applicable law and best practice.

The toolkit addresses the dual reality facing PSCs today: digital tools are indispensable for effective security operations, and the same tools can amplify harm if deployed without adequate safeguards. Each of the 12 tools in this toolkit addresses a specific technology domain, translating legal obligations and normative expectations into practical guidance for day-to-day operations.

1. Purpose and Objectives

The toolkit was developed to help private security companies:

- Understand how ICTs affect human rights in security operations and supply chains
- Navigate the growing body of law and regulation governing technology use — data protection, AI, cybersecurity, and labour rights
- Implement practical safeguards that meet legal obligations and reflect human rights best practice

- Engage with clients, regulators, and affected communities with credibility and transparency
- Align technology use with ICoCA certification requirements and the ICoC

2. Version 1.1: What's New

The toolkit was first published in November 2024. Version 1.1 updates all 12 tools to reflect significant regulatory and normative developments since that date. The table below summarises the key changes.

Regulatory Development	Key Change	Tools Updated
EU AI Act (Aug 2024; prohibitions Feb 2025)	Prohibited practices enforceable: RTBID in public spaces, emotion recognition in workplaces, biometric categorisation by sensitive attributes, social scoring. Annex III high-risk obligations (FRIA, conformity assessment, human oversight) mandatory from December 2027 (provisional — postponed by EU Digital Omnibus, May 2026).	Tools 1, 6, 7, 8, 9, 11, 12
CSDDD (Dir. (EU) 2024/1760; in force July 2024)	Mandatory HRDD for large companies; mandatory external grievance mechanisms; director accountability; phased from 2027.	Tools 9, 12
CSRD (mandatory from FY2024)	Large in-scope PSCs must publish sustainability reports with double materiality assessment covering ICT-related human rights impacts.	Tool 9
Pall Mall Process (endorsed April 2025, 25 states)	Primary international standard for responsible development, transfer, and use of commercial cyber intrusion tools.	Tools 6, 8
NIST PQC Standards (FIPS 203/204/205; August 2024)	First finalised post-quantum cryptography standards. 'Harvest now, decrypt later' attacks make migration planning a present obligation.	Tools 3, 4, 5, 8
EU Platform Work Directive (Dec 2024)	First EU law on algorithmic management: transparency rights, prohibition on emotional data processing in employment, human oversight of automated decisions.	Tool 11
EU Data Act (September 2025)	IoT data access rights; legal cloud-switching and deletion rights.	Tools 2, 3, 5
NIS2 Directive (transposed October 2024)	Mandatory 24h/72h incident notification; MSPs/MSSPs explicitly covered.	Tools 3, 4
ISO/IEC 27001:2022 (transition Oct 2025)	2013 edition now obsolete; 2022 edition restructures controls to 93 with new cloud and supply chain categories.	Tools 3, 4, 5
NIST CSF 2.0 (February 2024)	Adds Govern function; expanded scope beyond critical infrastructure to all organisations.	Tool 4
EDPB Opinion 11/2024	Centralised biometric databases with employer/PSC-held keys not GDPR-compliant; individual device-based storage required.	Tool 6
UN SR — AI & Counter-	Position paper calling for moratorium on AI systems	Tool 7

Regulatory Development	Key Change	Tools Updated
Terrorism (December 2025)	incompatible with international human rights law; guidance for PSCs using AI in security contexts.	

Why this update matters

The original toolkit described many of these frameworks as emerging, anticipated, or best practice. Version 1.1 reflects a fundamental shift: most of what was described as future law is now in force. For PSCs with EU operations, the EU AI Act's prohibitions have been enforceable since February 2025. Annex III high-risk AI obligations are mandatory from December 2027 (provisional — postponed by EU Digital Omnibus, May 2026). NIS2 incident notification timelines apply now. ISO/IEC 27001:2013 certification has expired. These are current legal obligations, not aspirational standards.

3. Structure and Navigation

The toolkit comprises this Intro document and 12 thematic tools:

Tool	Topic
Tool 1	Human Rights Challenges Posed by ICTs
Tool 2	Responsible Data Collection
Tool 3	Best Practices for Data Storage
Tool 4	Best Practices for Data Security
Tool 5	Best Practices for Data Destruction
Tool 6	Surveillance and Monitoring
Tool 7	AI-Enabled Decision-Making and Algorithmic Bias
Tool 8	Emerging Technologies and Offensive Cyber Capabilities
Tool 9	Due Diligence, Accountability, and Transparency
Tool 10	Freedom of Expression and Information
Tool 11	Workforce and Labour Rights in the Digital Age
Tool 12	Right to Remedy and Grievance Mechanisms

Companion Documents (Version 1.1)

- Regulatory-to-Tool Mapping: Cross-reference of regulatory frameworks to the tools where they are addressed, with monitoring sources and update triggers
- **Annex A — Master Reference List: All primary sources cited across the 12 tools**
- Annex B — Jurisdictional Applicability Guide: Which frameworks apply to which companies, with size and geography thresholds

- **Annex C — Master Glossary: Definitions of key terms used across the toolkit**
- **Annex D — Compliance Deadline Tracker: Chronological tracker of all regulatory deadlines**
- Annex E — Technology Decision Tree: Decision pathways for identifying applicable frameworks when deploying specific technologies
- Annex F — ICoCA Alignment Map: Maps toolkit tools to ICoC requirements and ICoCA certification standards
- Annex G — Country Comparison Table: Side-by-side comparison of data protection laws across key jurisdictions

4. How to Use this Toolkit

New users

Start with Tool 1 (Human Rights Challenges) for the conceptual framework, then navigate to the tools most relevant to your current technology deployments using the structure above or Annex E (Technology Decision Tree).

Users familiar with Version 1.0

Check the Version 1.1 Updates section at the top of each tool to see what changed and why. The updates are integrated into the body of each tool — the structure and navigation are unchanged.

ICoCA certification

Use Annex F (ICoCA Alignment Map) to navigate from ICoC chapters to the toolkit tools that address each chapter.

Compliance teams

Use Annex D (Compliance Deadline Tracker) for a chronological view of obligations, and Annex B (Jurisdictional Applicability Guide) to confirm which frameworks apply to your organisation.

Technology procurement

Start with Annex E (Technology Decision Tree) to identify applicable frameworks before procurement, then go to the relevant tool for detailed guidance.

The toolkit is available in full at boots2bytes.ch, where tools are searchable by topic and regulatory framework.

5. Normative Framework

The toolkit is grounded in the following foundational frameworks:

- UN Guiding Principles on Business and Human Rights (UNGPs): The three pillars — state duty to protect, corporate responsibility to respect, and access to remedy — provide the overarching structure for the toolkit's human rights approach
- International Code of Conduct for Private Security Service Providers (ICoC): The sector-specific normative standard for PSCs, operationalised through ICoCA certification. All 12 tools are aligned with ICoC requirements
- Montreux Document: The foundational intergovernmental document on PMSC obligations under international humanitarian law
- Voluntary Principles on Security and Human Rights: Relevant for PSCs operating in extractive industry contexts

- GDPR and national data protection law: The primary legal framework for data handling and privacy across the jurisdictions where most PSCs operate
- EU AI Act: The primary legal framework for AI governance, with global reach for any PSC deploying AI systems in or affecting EU individuals

6. Key Principles

All 12 tools are underpinned by five cross-cutting principles:

Proportionality

Technology use must be proportionate to the security objective. More capable or more intrusive technology is not inherently better — it must be justified by need, and the least intrusive effective option should be preferred.

Accountability

Someone must be responsible and answerable for every technology deployment. Automated systems do not distribute or dissolve accountability — they concentrate it in the people and organisations that deploy them.

Transparency

Affected individuals and communities have a right to know, in accessible terms, what technology is being used and how it affects them. This applies to clients, employees, and third parties.

Non-discrimination

Technology systems — especially AI — must be audited and monitored for discriminatory outputs. Algorithmic bias can produce systematic discrimination that is invisible to operators and deeply harmful to affected individuals.

Remedy

Where technology use causes harm, affected individuals must have access to effective remedy. Grievance mechanisms must be designed for the communities they serve, not the organisations that operate them.

7. Context: Technology and the Private Security Sector

Private security companies occupy a unique position in the digital age. They are among the most intensive users of surveillance, monitoring, biometric, and data technologies. They operate in complex environments — conflict-affected areas, critical infrastructure, multi-jurisdictional supply chains — where the consequences of technological failure are human, not merely operational. And they serve clients whose own regulatory obligations (particularly under CSDDD, the EU AI Act, and CSRD) flow downstream to their security service providers.

The past 18 months have confirmed that the regulatory gap which once allowed PSCs to operate with limited technology governance obligations is closing. The EU AI Act applies to deployers, not just developers. NIS2 explicitly covers managed security service providers. CSDDD creates supply chain obligations that reach to every significant subcontractor. The Pall Mall Process creates accountability expectations for companies offering or using commercial cyber intrusion capabilities.

The toolkit provides the practical foundation for meeting these obligations — not as a compliance exercise, but as an expression of the values that responsible private security companies hold: respect

for human rights, accountability for operations, and a commitment to transparency with those they serve and those they affect.

8. About this Toolkit

Developed by	ICT4Peace Foundation, Geneva, in collaboration with ICoCA
Version 1.0	November 2024
Version 1.1	June 2026
Online platform	boots2bytes.ch
Primary author	Anne-Marie Buzatu
Contact	ICT4Peace Foundation, Geneva