

Protecting Software IP

From source code to fiduciary duty.

External developers, contractors, offshore teams and AI coding agents now contribute to a growing share of enterprise software. Most organisations have no continuous visibility into who can access, modify, copy or expose their most valuable intellectual property — and across Europe, that gap is becoming a board-level legal duty.

BOARD DUTY

§ 93 AktG

Fiduciary duty to protect corporate assets

TRADE SECRETS

EU 2016/943

Protection only with "reasonable steps"

BOARD OVERSIGHT

NIS2

Personal liability for cyber governance

VALUE AT RISK

€100M+

Enterprise value tied to software IP

Under §93 AktG and equivalent EU corporate-governance law, management boards can face personal liability for failing to protect material corporate assets — increasingly software, algorithms, AI models and trade secrets.

EXECUTIVE SUMMARY

IP protection is now a board duty

For years, three risks were treated as separate problems: **IP theft** was a legal issue, **cybersecurity** was an IT issue, and **external developers** were a procurement issue. Today they converge. Under NIS2, the EU Trade Secrets Directive, national corporate-governance law and the emerging Cyber Resilience Act, boards are increasingly expected to demonstrate oversight of software assets, intellectual property, external developers, AI coding agents and software supply-chain risk.

This shifts the conversation from a security topic to a **governance, compliance and fiduciary-responsibility** topic — and raises a question most IP controls cannot answer: **can you prove who can access, modify, copy or expose the software that differentiates your company?**

THE LEGAL SHIFT IN EUROPE

From three separate problems to one fiduciary duty

HISTORICALLY — SEPARATE SILOS

- IP theft = a legal issue
- Cybersecurity = an IT issue
- External developers = procurement



TODAY — CONVERGED AT BOARD LEVEL

Boards have a fiduciary duty to protect material corporate assets.

- Software, algorithms, AI models & trade secrets are now among the most valuable.

WHAT IS AT STAKE

The risk, and the legal duty it now creates

KEY IP RISKS WITH EXTERNAL DEVELOPERS & AI AGENTS

**Source Code Exposure**

Code copied before departure, reused elsewhere, or reaching a competitor.

**Unauthorized Access**

Dormant accounts, contractor access after project end, shared credentials.

**Insecure Tools & Environments**

Unapproved tools and cloud services create uncontrolled leakage channels.

**IP Leakage via AI Tools**

Source pasted into AI assistants; prompts expose proprietary algorithms.

**Ownership Disputes**

Unclear contributor ownership, missing authorship evidence, weak governance.

THE EUROPEAN LEGAL LANDSCAPE · WHY BOARDS ARE NOW ACCOUNTABLE

§ 93 AktG — Duty of Care

GERMANY

Boards must protect material corporate assets — including source code, algorithms, AI models and trade secrets.

GeschGehG — Trade Secrets

GERMANY

Protection applies only with "appropriate secrecy measures." Weak controls can forfeit legal protection.

NIS2 Directive

EU-WIDE

Management bodies must approve, oversee and be accountable for cyber-risk measures, with personal liability.

Trade Secrets Directive

EU 2016/943

Trade secrets are protected only where the company took "reasonable steps" to keep them secret.

Cyber Resilience Act

EU

Secure-by-design SDLC and product-cybersecurity accountability — who changed, approved and deployed code.

Code de Commerce

FRANCE

Director fiduciary duties; the Loi de Vigilance extends risk oversight across the supplier & developer chain.

Burgerlijk Wetboek

NETHERLANDS

Directors must properly manage the company; failure to protect valuable assets can create liability.

Codice Civile / LSC

ITALY & SPAIN

Directors must act with due diligence to preserve corporate value, including know-how and source code.

TRADITIONAL IP PROTECTION ANSWERS

Who owns it — on paper?

NDA · Contract · DLP · Source-code escrow

Defines ownership and intent, but not who can actually reach the code.

BLUEFLAG ANSWERS

- ✓ Which external developers have access?
- ✓ Which repositories, branches & secrets?
- ✓ Which CI/CD pipelines?
- ✓ Which AI coding agents?
- ✓ Can you prove governance?

WHERE BLUEFLAG FITS

The hardest question: who can reach your IP?

Traditional IP controls — NDAs, contracts, DLP and escrow — define ownership on paper. They cannot show who can actually access, modify, copy or expose the code in practice across employees, contractors, third-party developers, machine identities and AI coding agents. BlueFlag is the governance, visibility and control layer that can.

1 Developer Identity Governance

- Who has access — and which repositories, branches and secrets
- Least-privilege & just-in-time access
- Strong authentication & device trust
- Continuous access review

IP VALUE

"Which external developers can reach our code?" — answered continuously.

2 Code & Data Protection

- Secure repositories with granular permissions
- Data-loss prevention on code movement
- Encryption in transit and at rest

IP VALUE

Detect unusual code movement before IP leaves the organisation.

3 Controlled Dev Environments

- Isolated, ephemeral environments
- No local code storage
- Prevent copy / paste / download / screenshots

IP VALUE

Contractors build without code ever leaving a governed boundary.

4 Third-Party & Tool Security

- Vet and monitor third-party tools
- Restrict unapproved services
- Secure integrations and APIs

IP VALUE

Close the uncontrolled channels through which IP quietly leaks.

5 IP in AI & Automation

- Which AI tools are in use — Claude Code, Cursor & others
- Block sensitive code from AI tools
- Monitor and audit AI tool usage

IP VALUE

"Who connected which AI agent, and what did it touch?" — answerable.

6 Governance & Compliance

- Clear IP-ownership definitions & strong clauses
- Audit trails and compliance reporting
- Demonstrable separation of duties

IP VALUE

Prove the "reasonable steps" that trade-secret protection now requires.

COMPLETE VISIBILITY ACROSS THE ACCESS CHAIN

Developer > Repository > Branch & Secret > CI/CD Pipeline > AI Agent

MAPPING: BOARD / LEGAL QUESTION → BLUEFLAG EVIDENCE

Obligation	What boards / auditors / acquirers ask	BlueFlag evidence
Trade-secret protection	Did we take "reasonable steps" to keep it secret?	Access governance, permission reviews, and proof that access was removed after project end.
Board fiduciary duty	Are our most valuable software assets governed?	Attributable inventory of every developer, machine identity and AI agent across the SDLC.
External-developer risk	Who can access, modify or copy our code?	Identity-correlated view across source control, repositories, secrets and pipelines.
AI governance	Is AI coding-tool usage controlled?	AI agent inventory, AI identity tracking and code-to-AI exposure monitoring.
M&A / PE due diligence	Can we prove our IP is adequately protected?	Exportable IP-governance evidence and a pre-acquisition readiness view.

BlueFlag Security · Intellectual Property Protection · Solution Brief

blueflagsecurity.com · June 2026 · Page 3 of 4

HOW BLUEFLAG WORKS

Connect, discover, detect, remediate — no agent, no code changes

1

CONNECT

Pre-built API integrations across source control, CI/CD, IAM, registry and SIEM. Deployed in under 30 minutes — no agent, no code changes.

2

DISCOVER

Continuously inventory every developer — human, non-human and AI agent — and every dev-tool activity into one identity graph with behavioural baselines.

3

DETECT

Surface excessive permissions, dormant contractor accounts, access after contract end, privilege escalation and unusual code movement — with full identity context.

4

REMEDiate

Enforce policy in real time — right-size access, govern AI tool usage, and generate audit-ready evidence of IP protection.

THE BUSINESS VALUE

Protecting the assets that differentiate the company



Protect proprietary code & algorithms

Trading algorithms, control software, AI models and roadmaps that represent the company's core value.



Maintain competitive advantage

Keep the differentiating software inside the organisation, governed across people, machines and AI.



Reduce IP-theft & legal risk

Demonstrate the "reasonable steps" trade-secret law requires and reduce board-liability exposure.



Preserve enterprise & M&A value

Provide due-diligence-ready evidence; a material IP-leakage incident directly impacts valuation.

WHY THE C-SUITE & BOARD SHOULD CARE

CISO / CSO

A board-defensible, attributable inventory of every developer, contractor, machine identity and AI agent that can reach source code — with policy enforced in real time, not aspirational.

CIO / CTO

Operationalise external and AI-driven development safely and at scale — govern who and what can access the code without slowing engineering down.

CFO

Protect the software assets that carry hundreds of millions of euros of enterprise value, and reduce the breach, liability and valuation exposure of IP loss.

General Counsel / GRC

Demonstrate the "reasonable steps" and separation of duties required under the Trade Secrets Directive, §93 AktG, NIS2 and the CRA — with exportable evidence.

Board / PE Investor

Answer the fiduciary question directly: can we prove our most valuable software assets are adequately protected, before and after acquisition?

EXECUTIVE MESSAGE

"Under §93 AktG and equivalent EU corporate-governance law, management boards have a fiduciary duty to protect the company's most valuable assets. Today those assets are software, algorithms, AI models and trade secrets. BlueFlag Security provides continuous visibility and governance over who can access, modify, copy or expose them — across employees, contractors, third-party developers, machine identities and AI coding agents."

Raj Mallempati · CEO & Founder, BlueFlag Security