

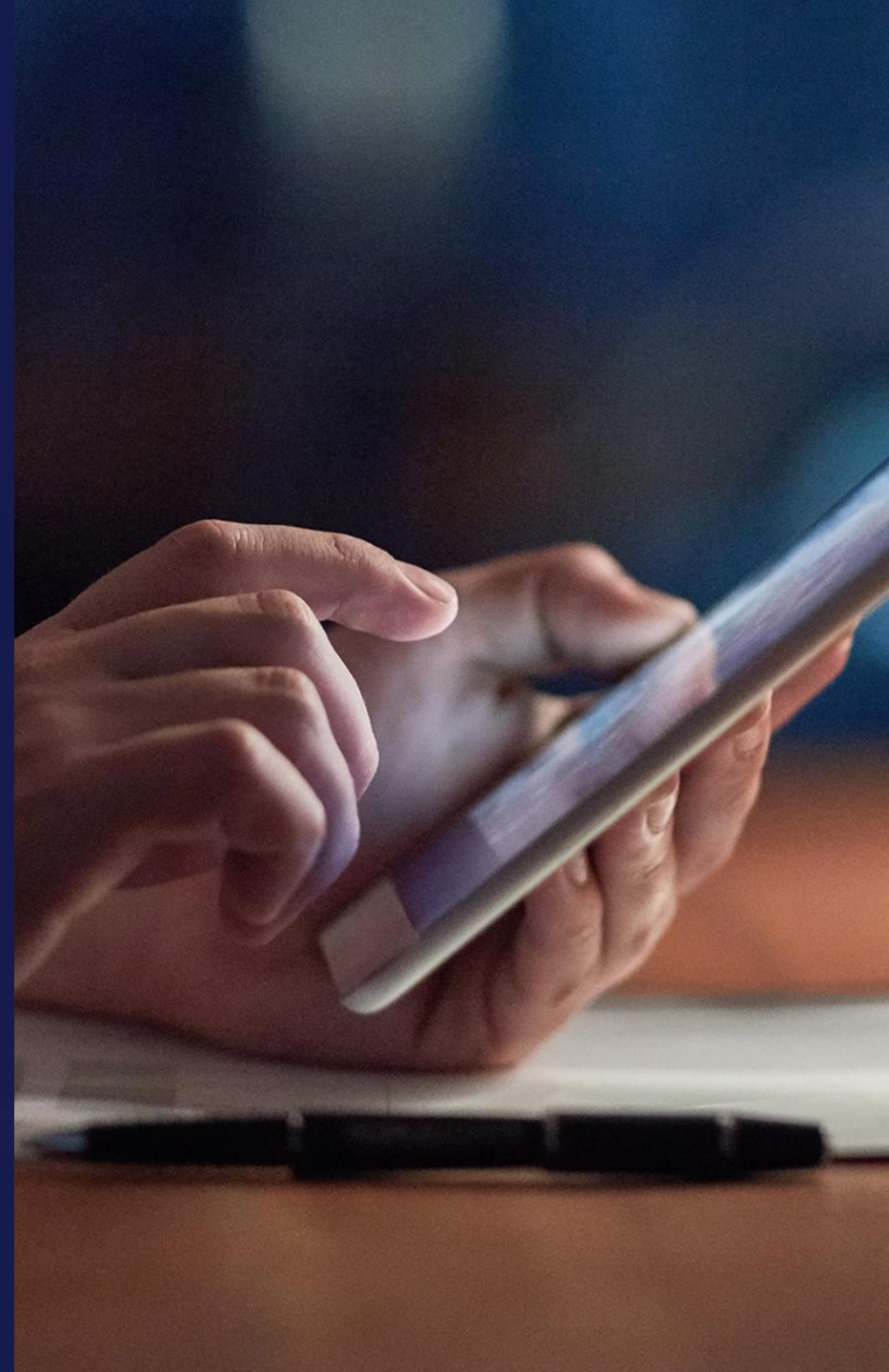
IP Protection in Ukraine

Trademarks, Patents, Copyrights, Enforcement

Ukraine 101: Monthly Legal Basics | AHK Ukraine

Vasyl Pop-Stasiv, LL.M.
Counsel, Head of IP/IT | Taylor Wessing Ukraine

2026



Three questions for legal teams

A practical rather than encyclopaedic approach



Protect

Do we actually own and control the IP,
brand and know-how we rely on?

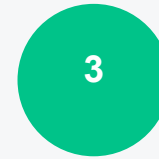
Employees • contractors • distributors



Maintain

Are our rights still alive, defensible and
supported by evidence?

Renewals • non-use • portfolio hygiene



Enforce / regulate

Which tool works in practice — and when
does IP law stop being enough?

Enforcement • defence • dual-use

The objective: one group-wide IP strategy, with Ukrainian execution where local law or practice requires it.

IP protection is a system — not a certificate

The filing is only one part of the control environment

1 Ownership

Can we prove the chain of title from the creator to the current rights holder?

2 Scope

Do registrations, contracts and licences cover the actual products, territories and uses?

3 Evidence

Can we prove creation, use, confidentiality and infringement when challenged?

4 Enforcement

Do we have a realistic route to stop the conduct — quickly and proportionately?

A strong portfolio with a weak chain of title or weak evidence can still be a weak asset.

Ownership starts with the chain of title

Do not assume one rule covers every type of IP



Key legal distinction

Copyright works: economic rights in an employee-created work transfer to the employer, and rights in a commissioned work transfer to the customer, unless the contract or law provides otherwise. **Other IP objects:** do not automatically follow the same rule; patents, utility models, designs and know-how require object-specific analysis.

Practical rule: map the asset → identify the creator → identify the legal basis for vesting/transfer → keep the evidence.

The safest group structure is the one you can prove, not merely the one shown in the organigram.

Employees and contractors: where ownership breaks

The recurring problem is usually evidence and scope, not the absence of an “IP clause”

Risk trigger	Why it matters	What legal should do
Unclear duties / deliverables	Harder to prove that the specific output was created within employment or under the commission	Define expected creative / technical outputs and retain task records
Background IP mixed with new work	The company may receive less than it thinks it commissioned	Schedule pre-existing tools, libraries, code and know-how
Open-source or third-party content	Licence terms can restrict distribution or require disclosure	Require disclosure, approval and licence-compliance process
Group company is not the contracting party	Ownership chain may stop at the Ukrainian entity	Build assignment / licence route deliberately and document it
Exit without handover	Source code, credentials, repositories and evidence can leave with the individual	Make IP handover part of offboarding, not an afterthought

Distributors and commercial partners: control the exit

Many brand disputes start after the commercial relationship has already failed

Before launch

- Trademark / domain clearance
- Who owns local domains and social accounts?
- Permitted brand use and territory
- No filings in partner's own name

During the relationship

- Approved marketing materials
- Marketplace / reseller controls
- Monitoring of confusingly similar filings
- Evidence of authorised use

At exit

- Immediate cessation mechanics
- Transfer of domains / accounts / materials
- Stock sell-off rules
- Post-termination monitoring

Grey-market reminder

Trademark law is not a general distribution-control tool: genuine goods placed on the market by the owner or with consent may trigger exhaustion, subject to legitimate reasons to oppose further commercialisation.

Know-how and trade secrets: an NDA is only one layer

Protection depends on how the business actually treats the information

1. Secret

Not generally known or readily accessible to the relevant circle.

2. Commercial value

Value exists because the information remains secret.

3. Adequate measures

The holder must take measures that are adequate in the circumstances to preserve secrecy.



If everyone can access it, “Confidential” in the footer will not create a trade secret.

Martial law continues — the special IP deadline regime does not

This distinction is now a portfolio-management issue



Do not use the continued existence of martial law as a proxy for continued deadline relief.

Portfolio audit: what should be checked now?

A practical 2026 checklist for international groups



Renewals & annuities

Any right that relied on wartime extensions?



Ownership & recordals

Does the register still match the group structure?



Actual use

Can you evidence use for the goods / services that matter?



Madrid vs national rights

Are designations aligned with the commercial portfolio?



Watch / oppositions

Are former partners or competitors filing similar marks?



Domains & online assets

Who controls .ua domains, seller accounts and social profiles?

A one-off “post-war” audit is too late: the relevant deadlines and non-use periods are already running.

Trademark non-use: the statutory period is five years

War may be relevant to justification — but it is not an automatic safe harbour

5 YEARS

continuous non-use can
expose a Ukrainian trademark
registration to early
termination, in whole or in part.

1

Use must be genuine

Check use against the registered goods/services, not merely general brand visibility.

2

Permitted use counts

Use by another person with the owner's consent can qualify.

3

Valid reasons are fact-specific

The law recognises circumstances independent of the owner, including import restrictions or regulatory requirements.

4

Evidence should be built before the dispute

Invoices, imports, advertising, website records, distributor evidence and market documentation.

The practical question is not “Did the war happen?” but “Can we prove why this mark could not reasonably be used, and for how long?”

Enforcement: choose the route by objective

The “strongest” remedy is not always the best first remedy

Route	Best for	Typical advantage	Main constraint
Platform / host takedown	Online listings, marketplace abuse	Speed; low procedural burden	Platform rules and repeat sellers
Cease & desist / negotiation	Identifiable commercial infringer	Fast leverage; settlement potential	Depends on counterparty incentives
Customs border measures	Counterfeit imports / exports	Stops goods at the border	Needs right identification and operational follow-up
Civil litigation	Injunction, damages, invalidity / ownership disputes	Binding relief and precedent value	Time, evidence, cost and enforcement strategy
Police / criminal route	Counterfeiting and conduct meeting criminal thresholds	Investigative powers	Thresholds, prioritisation and case management

Enforcement during wartime: same toolbox, different sequencing

The legal mechanism is only one input into the business decision

Speed

How quickly must the conduct stop?

Evidence

Can we preserve seller, platform, payment and shipment evidence now?

Economics

Is the commercial harm proportionate to the cost of escalation?

Reputation

Could enforcement against a local partner, volunteer-linked business or strategic supplier create wider issues?

Continuity

Will the remedy disrupt supply, service or reconstruction / defence-related operations?

Recoverability

Is damages recovery realistic, or is injunctive relief the real objective?

Local context should change the enforcement strategy — not eliminate enforcement as an option.

EU harmonisation: align the strategy, localise the execution

Increasing legal convergence does not eliminate Ukrainian-specific risk

What can be aligned

- Group ownership principles
- Portfolio taxonomy and clearance process
- Standard licence / distribution controls
- Evidence-retention standards
- Escalation matrix for enforcement



What still needs local execution

- National registrations and procedural deadlines
- Ukrainian-language evidence and local filings
- Object-specific ownership rules
- Local enforcement economics and counterparties
- Export-control / security overlays in regulated sectors

The goal is not “EU template vs Ukrainian template”; it is one control framework with deliberate local adaptations.

Technology protection beyond IP

In strategic sectors, ownership can be clear and the transfer can still be restricted

IP RIGHTS

patents • copyright • designs • trade secrets • licences

CONTRACTS

background / foreground IP • use rights • access • confidentiality • exit

EXPORT CONTROL

military / dual-use goods, software, technology and technical assistance

SECURITY / SECRECY

state secrets • restricted publication • access and disclosure rules

STATE / PROCUREMENT LAYER

defence procurement • state funding • contractual use / access rights

“Who owns it?” and “May we disclose, export or commercialise it?” are separate questions.

Defence / dual-use: five questions before sharing technology

Use this checklist before the NDA, data room or cross-border R&D call

1

What is it?

Military, dual-use, civilian — and could catch-all controls apply?

2

Who owns it?

Background IP, new developments, employee / contractor contributions, state-funded elements.

3

Who may receive it?

Entity, jurisdiction, end-user and internal group recipient.

4

What is the transfer?

Physical item, source code, technical documentation, remote access, technical assistance.

5

What approvals / restrictions apply?

Export-control permit, secrecy classification, procurement or security conditions.

Do the regulatory classification before the technology leaves the controlled environment — not after.

Five actions for legal teams — and Q&A

A practical closing checklist

1

Audit renewals, ownership records and evidence of trademark use.

2

Trace chain of title for high-value software, technology and content.

3

Build distributor / contractor exit mechanics into the contract before the relationship deteriorates.

4

Treat trade secrets as an operational control system, not just an NDA.

5

For defence / dual-use projects, run IP and regulatory analysis in parallel.



Vasyl Pop-Stasiv, LL.M.

Counsel, Head of IP/IT
Taylor Wessing Ukraine
v.pop-stasiv@taylorwessing.com