pescheck

INDUSTRY BRIEF

Personnel Screening in Deep-Tech, Defence & Aerospace

How security-sensitive organisations can hire faster without lowering the security bar.

Deep Tech

Semiconductors

Photronics

Advanced Manufacturing

Export-Controlled Environments

ATG europe

RENK

EUMETSAT

STARK

TYTAN TECHNOLOGIES

ARX ROBOTICS

NATO OTAN

Europe is Hiring at Speed in its Most Sensitive Sectors

European defense, space and deep-tech is in the middle of its fastest expansion in decades. The EU's ReArm Europe plan proposes unlocking up to €800 billion in defense investment, supported by new mechanisms such as the Security Action for Europe (SAFE) facility.[1] EU defense spending rose by around 60% between 2020 and 2025.[2]

Numbers

The industrial base is straining to keep up. ASD Europe puts employment in the European defense industry at roughly 581,000 people, with job postings still more than 40% above pre-2022 levels.[3] Recruitment timelines of six to nine months for senior technical and operational profiles are commonplace across the sector, and the gap is widest for exactly the profiles deep-tech programmes depend on: dual-use CTOs, programme directors, and cybersecurity and digital transformation leads.[1] Industry representatives also note that recruiting from outside political and strategic alliances is effectively off the table for large defense employers, even where the skills base is strong, which shrinks the available pool further.[4]

At the same time, the security bar for each of those hires has risen. The Dutch intelligence service AIVD warns that companies, research institutions and government in the Netherlands hold knowledge and technology that cannot be obtained at that level anywhere else in the world, naming quantum technology and semiconductors among the examples and describing these as the country's technological "crown jewels".[5]

Its assessments identify the recruitment of Western scientists and employees of high-tech firms as one of the primary acquisition methods, alongside cyber operations and corporate acquisitions.[6] In an earlier case, the AIVD disrupted a Russian SVR officer who had built a substantial network of sources working in the Dutch high-tech sector, with interests spanning artificial intelligence, semiconductors and nanotechnology.[7]

This is not theoretical for employers. ASML disclosed that a former China-based employee had misappropriated data relating to proprietary technology, in an incident the company said may have violated certain export control regulations.[8] Dutch reporting subsequently indicated the individual went on to work at Huawei.[9] In April 2026, two men were sentenced in the US for facilitating a "laptop farm" that placed North Korean IT workers inside more than 100 companies using 80+ stolen identities, a scheme that included the theft of export-controlled data from a California defense contractor.[10] The control that failed there was identity verification at the point of hire, not the firewall.

The candidate side of the market is shifting too. Gartner research has projected that by 2028 roughly one in four candidate profiles globally could be fake, built from stolen identities, AI-generated audio and video, or a combination.[11] Formal background checks already surface discrepancies against what the candidate claimed in an estimated 20–30% of cases.[12]

The result is a squeeze every HR and security lead in this sector recognises: hire faster than ever, from a smaller and more constrained talent pool, with more to lose if you get it wrong.



Why Screening is Now a Compliance Requirement, not a Nice-to-Have

For deep-tech, defense and aerospace employers, personnel screening sits at the intersection of several regulatory regimes at once:

- **EU Dual-Use Regulation (EU) 2021/821.** Export controls cover not only hardware and software but technical knowledge. This includes engineering specifications, manufacturing processes, research data, design blueprints and source code. Granting an employee access to controlled technology can therefore carry export control obligations. Failure to comply risks regulatory investigations, financial penalties, loss of government contracts and restrictions on international business activity.[13]

- **NIS2 and its implementing regulation.** Article 21(2)(i) makes human resources security an explicit cybersecurity risk-management measure.[14] The implementing rules (Commission Implementing Regulation (EU) 2024/2690, §10.2.2) call for verification appropriate to the role completed before access is granted. NIS2 does not mandate government-grade clearances; scope is proportionate to role risk and asset classification.[15]

- **ISO/IEC 27001:2022, control A.6.1.** Background verification must be carried out on all candidates before joining and on an ongoing basis, proportional to the classification of information to be accessed and the perceived risks.[16] In practice, auditors expect a screening policy, a role risk-classification matrix, and a documented screening record per person with screening depth that increases when someone moves into a more sensitive role.[17]

- **Clearance and programme requirements.** NATO member-state eligibility rules, national clearance regimes, ESA and EASA programme conditions, and customer-imposed restrictions in prime–supplier chains each add their own documentation burden.

- **GDPR.** All of the above must be lawful, data-minimised and defensible, with particular care around criminal-record data under Article 10.

Screening here therefore has to satisfy two audiences that usually pull in opposite directions: security and compliance teams who want depth and evidence, and hiring managers who cannot afford to lose a scarce engineer because vetting took three weeks.

PESCHECK helps organisations translate personnel-security and compliance requirements into consistent, role-based screening workflows across countries, entities and systems.

Matching Screening Depth to Role Risk



Screening depth: Cleared

Systems engineer on a defence programme for a prime contractor

This engineer works under contractual security requirements set by the prime and the government customer. The role may involve access to classified information.

Screening: the standard package, plus international criminal record checks for previous countries of residence, an adverse media check, an integrity declaration, and periodic rescreening during the contract.



Screening depth: Standard

Embedded software engineer at a dual-use sensor scale-up

This engineer has access to proprietary source code and product roadmaps, but not to classified information. The main risks are misrepresented skills or experience, and IP leaving the company with a departing employee.

Screening: identity verification, education verification, employment history, references, a VOG with a role-appropriate screening profile, and a sanctions check.



Screening depth: Enhanced

Research scientist working with export-controlled technology

This scientist has access to controlled technology, for example in advanced materials, quantum or propulsion. The key risks are unauthorised technology transfer, including intangible transfer through knowledge and data, and undisclosed ties to foreign entities.

Screening: the cleared package, plus in-depth sanctions and PEP screening and, where lawful and proportionate, a financial check

What is Actually Possible to Verify

A well-designed programme starts from the risk, not the check. Every role carries a baseline risk of misrepresented identity, qualifications or work history. Cleared roles add exposure to criminal records and financial vulnerability. Roles touching export-controlled technology add the risk of sanctions violations and undisclosed foreign ties.

Each tier therefore gets a different depth of screening, matched to what could actually go wrong in that role. Pescheck supports the full range, from standard verification to in-depth checks for the most sensitive positions [18].

- Identity fraud → Identity & biometric verification
- Insider / integrity risk → Integrity declaration, adverse media
- Export-control exposure → Relevant declarations and documentation
- Qualification risk → Education and certification verification
- Experience risk → Employment and reference verification
- Sanctions exposure → Sanctions / PEP / watchlist screening
- Ongoing personnel risk → Periodic or event-based re-screening

The Pescheck Case

The challenge our customers brought us

- Strict security and eligibility requirements, including international hiring constraints across NATO member states
- High hiring volume across multiple regions, entities and organisational types
- Manual, decentralised screening that differed by division and did not scale
- Enterprise and government clients demanding full traceability and auditability
- Compliance obligations spanning export control, clearance, NIS2 and ISO 27001 simultaneously

What we implemented

- Standardised screening workflows per role tier, so the same evidence is collected the same way in every country and business unit
- Security-focused check packages covering clearance-track requirements, export-compliance documentation and sanctions screening
- ATS and system integration, including Taleo and Oracle, alongside 100+ other integrations and a full API, so screening starts automatically from the existing recruitment process [18]
- Centralised dashboard with live status per candidate, structured decision-making and a complete audit trail
- EU-built, EU-hosted infrastructure, ISO 27001 and NEN 7510 certified, POB/WPBR registered and PBSA affiliated [19]

The outcome

- Designed to support a compliant, audit-ready screening process, with each step documented so decisions can be explained to regulators, auditors and prime contractors
- Average turnaround of under 4 hours, against sector recruitment cycles measured in months [18]
- A consistent screening standard across teams, entities and countries, helping reduce variation between divisions
- A partnership running since 2020, across more than 300,000 screenings performed on our technology for 2,600+ organisations [18]

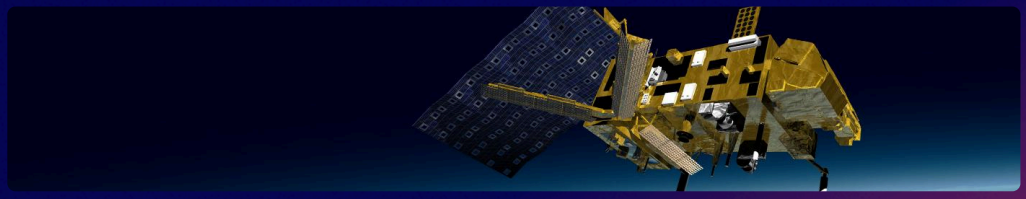
ATG europe · RENK · EUMETSAT · STARK · TYTAN TECHNOLOGIES · ARX ROBOTICS · NATO OTAN

Why it Matters Commercially, not Just Legally

Screening is increasingly a condition of doing business in this sector. Primes audit their suppliers' personnel security, government customers require demonstrable vetting, and investors in dual-use deep-tech ask how IP is protected. At the same time, you need to hire highly specialised people quickly, before they accept another offer. PESCHECK sits exactly between those two needs. A documented, standardised programme keeps hiring moving and turns a compliance cost into a credential you can put in front of a customer.

The economics hold up independently. Around 10% of candidates show a background discrepancy, and a bad hire can cost up to 2.5x their salary [18], before accounting for a lost contract or a compromised research programme. At the extreme end, breaches caused by malicious insiders are the most expensive category, averaging $4.99 million per incident [20]. Speed matters, but not at the expense of security.

Organisations in this sector working with Pescheck include NATO, ESA, EUMETSAT, the Dutch Ministry of Defence, ATG Europe, RENK, STARK, TYTAN Technologies, ARX Robotics, Black Semiconductor, Deep Tech Lab Quantum, Lobster Robotics and Avantgarde.



Sources

1. CE Interim, European Defence Industry: The Next 25 Years (June 2026) — ReArm Europe and SAFE, €800bn, 6–9 month recruitment timelines, skills gap by profile. https://ceinterim.com/european-defence-industry-outlook-next-25-years/

2. 2020s European rearmament — EU defense spending +60%, 2020–2025. https://en.wikipedia.org/wiki/2020s_European_rearmament

3. Patria, Wanted: European defence sector talent (June 2026), citing ASD Europe — ~581,000 employees; postings 40%+ above pre-war levels. https://www.patriagroup.com/newsroom/patria-magazine/situation/wanted-european-defence-sector-talent

4. ASD Europe, Intense search for skilled workers as Europe's defence industry demand outpaces talent supply — recruiting outside political and strategic alliances effectively impossible for large firms. https://www.asd-europe.org/news-media/news-events/news/intense-search-skilled-workers-europe-defence-industry-demand-talent-shortage/

5. Delta (TU Delft), The AIVD continues to warn against the theft of knowledge (April 2026) — AIVD annual report; "crown jewels"; quantum and semiconductors. https://delta.tudelft.nl/en/article/the-aivd-continues-to-warn-against-the-theft-of-knowledge

6. CISO Community Nederland, summary of the AIVD 2024 annual report — recruitment of Western scientists and high-tech employees as an acquisition method; first joint AIVD/MIVD public attribution of a cyberattack on a Dutch defense network to the Chinese state. https://www.cisocommunity.nl/news/219-offensive-cyber-operations-on-the-rise-aivd-2024-annual-report

7. AIVD (official), AIVD exposes espionage network in the Netherlands — SVR officer's source network in the Dutch high-tech sector; AI, semiconductors, nanotechnology. https://english.aivd.nl/latest/news/2020/12/10/aivd-exposes-espionage-network-in-the-netherlands-two-russian-intelligence-officers-forced-to-leave-the-country

8. CNBC, ASML says ex-China employee misappropriated data relating to its critical chip technology (Feb 2023). https://www.cnbc.com/2023/02/15/critical-chip-firm-asml-says-former-china-employee-misappropriated-data.html — see also CNN: https://edition.cnn.com/2023/02/15/tech/asml-china-employee-data-breach-intl-hnk

9. South China Morning Post, Employee of chip equipment giant ASML accused of stealing company secrets went to Huawei (Oct 2023), citing NRC. https://www.scmp.com/tech/tech-war/article/3239008/employee-chip-equipment-giant-asml-accused-stealing-company-secrets-went-huawei-report

10. Insider Risk Index, Insider Threat Incidents 2026 (June 2026), summarising DOJ records — April 2026 sentencings; 80+ stolen identities; 100+ companies; export-controlled data taken from a California defense contractor. https://www.insiderisk.io/research/insider-threat-incidents-2026

11. Avvanz, Resume Fraud in 2026, citing Gartner — roughly 1 in 4 candidate profiles potentially fraudulent by 2028. https://www.avvanz.com/blog/resume-fraud-2026-employer-prevention (secondary source — cite the original Gartner research if you can obtain it)

12. Octagnt, What the resume fraud statistics 2026 actually say — 20–30% of formal background checks surface a discrepancy. https://www.octagnt.ai/blog/what-the-resume-fraud-statistics-2026-actually-say-will-make-you-rethink-your-last-five-hires/

13. Pescheck, Export Control Compliance for Tech Hiring in Europe (Sept 2026) — Regulation (EU) 2021/821 scope including technical knowledge; consequences of non-compliance. https://pescheck.io/blog/export-control-compliance-for-tech-hiring-in-europe-a-complete-guide-for-hr-and-recruitment/

14. Resiliently, NIS2 Article 21 Technical Measures (April 2026) — Art. 21(2)(i) covers personnel security including background screening; Art. 20 governance and management liability. https://resiliently.ai/blog/posts/nis2-article-21-technical-measures-security-requirements-2026

15. NIS2-Templates, NIS2 Access Control and Human Resources Security: Article 21(2)(i) (May 2026) — CIR 2024/2690 §10.2.2 verification scope and pre-access timing. https://www.nis-2-templates.com/access-control/ — see also ISMS.online: https://www.isms.online/nis-2/implementing-guidance/hr-security/10-2/

16. ISMS.online, ISO 27002:2022 Control 6.1 – Screening. https://www.isms.online/iso-27002/control-6-1-screening/

17. Indicium, ISO 27001:2022 Annex A.6.1 personnel vetting (May 2026) — full A.6.1 control text, audit evidence expectations, role risk-classification matrix, re-screening on role change. https://www.indicium.ag/en/resources/iso-27001-annex-a6-personnel-security-2026

18. Pescheck. Platform capabilities and figures: 31,000+ ID documents, check catalogue, 100+ integrations and API, <4h average turnaround, 300,000+ screenings, 2,600+ organisations, ~10% discrepancy rate, bad hire up to 2.5x salary. https://pescheck.io/

19. Pescheck, Aerospace Industry Background Checks. Sector customer logos, ISO 27001 and NEN 7510, POB/WPBR registration, PBSA affiliation, export compliance certification checks, clearance-aligned screening. https://pescheck.io/industry/aerospace/

20. Bright Defense, Risks and Mitigation of Insider Threats, citing Ponemon Institute — malicious insider breaches average $4.99m per incident. https://www.brightdefense.com/resources/risks-and-mitigation-of-insider-threats/