EU READY STARTUPS LAB

2026 PROGRAM

BY INNOVATION NEST

PROGRAM MANUAL

Prepared by Innovation Nest

September 2026

About This Manual

This manual brings together the three working sessions of the EU Ready Startups Lab — 2026 Program, held on 10 September 2026 at Piramida, Tirana. It is organised as a practical reference in three parts, one for each session, so that founders and teams can return to the material after the event and use it as a working checklist rather than a set of slides.

Each part follows the structure of its original session and closes with an action checklist and key takeaways. Legal references, dates and figures are reproduced as presented in the sessions; readers should verify current requirements against the official texts and the Commissioner's or relevant authority's guidance before acting on them.

The Three Parts

- Part I — Green Business Models & Circular Economy: Selling into the EU in 2026
- Part II — GDPR: Law No. 124/2024, Personal Data Protection in the Age of AI
- Part III — AI and Cybersecurity Standards: What Startups Need to Know for the EU Market

PART I — Green Business Models & Circular Economy

Selling into the EU in 2026: the four gates your green claim has to pass

1. Purpose and Roadmap of This Session

This session moves from the fundamentals of the circular economy to what specifically changed in EU and Albanian rules during 2026 and closes with a hands-on clinic applying the rules to real claims from Albanian products.

The session runs in three blocks:

- **Foundations (≈ 20 min)** what circular economy really means, five business models, and European startups that make money from it.
- **The 2026 update (≈ 22 min)** what changed since the reference guide was written, and the four regulatory "gates" standing between a startup and the EU market.
- **Green Claim Clinic (≈ 15 min)** a readiness self-assessment, followed by a live rebuild of real environmental claims.

> *Two starting questions are used to gauge the room and are worth answering for your own business before reading on:*
>
> *(1) Do you sell, or plan to sell, to a customer in the EU directly, online, or as a supplier to an EU company?*
> *(2) Does the word "eco", "green", "bio", "natural" or "sustainable" appear anywhere on your product, packaging or website? If you answered yes to the second question, Part I, Section 4 (Gate 1) applies to you directly.*

2. Foundations: What Circular Economy Really Means

2.1 From a Straight Line to a Loop

The economy most businesses inherited is linear: take → make → use → waste. Virgin resources are extracted, manufactured, sold, used often once or briefly, then landfilled or incinerated losing their value. This worked only while resources appeared infinite.

The EU has decided this model ends. The European Green Deal (2019) and the Circular Economy Action Plan (2020) turned circularity from a value into law. Albania is negotiating the same rulebook through Chapter 27 (Environment) of the EU accession acquis, and its own Extended Producer Responsibility (EPR) law now mirrors the EU's. The question for a startup is therefore not whether these rules arrive, but which rule reaches it first.

2.2 Circular Economy in Three Principles

Using the Ellen MacArthur Foundation framing:

- **Eliminate waste and pollution** - design them out from the start. Waste is a design failure, not a fact of life.
- **Circulate products and materials** - keep them in use at their highest value: maintain, reuse, refurbish, remanufacture - recycle only as a last resort.
- **Regenerate nature -** return nutrients and restore soil and ecosystems, instead of only doing "less harm".

2.3 Two Loops: Biological and Technical

Which loop a product belongs to decides its whole business model.

- **Biological cycle** - materials that can safely return to nature: food, fibre, wood, bio-based packaging. Loops: compost, biogas, regenerative farming, cascading uses. Albanian fit: agro-processing, olive, herbs, natural-fibre textiles.
- **Technical cycle** - materials that must be kept out of nature: metals, plastics, electronics, machinery. Loops: maintain → reuse → refurbish → remanufacture → recycle. Albanian fit: footwear, furniture, e-waste, construction materials.

2.4 The R-Ladder: Recycling Is Step 9 of 10

The higher the step on the ladder, the more value is kept — and the less it costs. In order of preference: Refuse, Rethink, Reduce (smarter product use and manufacture), Reuse, Repair, Refurbish, Remanufacture, Repurpose (extending product lifespan), Recycle, Recover (useful application of materials, the last resort).

> *In an Albanian survey behind this session's reference guide, 70% of respondents named recycling as the key element of circularity. Recycling is the safety net, not the strategy - a startup that starts its circular story with "we recycle" is starting on the wrong rung of the ladder.*

2.5 The State of Readiness (Survey Data)

From a survey of young entrepreneurs, startups, MSMEs and consumers underpinning the reference guide (2024):

- 65% recognise sustainability as crucial to their business model.
- 40% feel equipped to put circular principles into practice.
- 60% of startups struggle to turn principles into a concrete strategy.
- 85% believe the circular economy has a positive impact on climate

The gap between the 65% who value sustainability and the 40% who feel equipped to act on it is the reason structured guidance — and this session — exists.

3. Circular Business Models and European Examples

3.1 Four Ways to Build a Circular Business

Three of the four categories below come directly from the reference guide's business-model chapter; the fourth, "Enable", is a category that grew after the guide was written.

- **Narrow the loop (circular supplies / resource efficiency)** use less per unit. Examples: Sulapac (Finland), a wood-based material replacing plastic packaging; Orbisk (Netherlands), a camera-and-AI system that cuts food waste in professional kitchens.
- **Slow the loop (product life extension / product-as-a-service / sharing platforms)** use longer. Examples: Back Market (France), a refurbished-electronics marketplace; Swapfiets (Netherlands), a bike subscription where the company owns the bike; Vinted (Lithuania), Europe's largest resale market.
- **Close the loop (resource recovery / take-back & remanufacture)** use again. Examples: Too Good To Go (Denmark), surplus food sold before it becomes waste; Fairphone (Netherlands), a modular phone with parts recovered and reused.
- **Enable the loop (traceability & passports / carbon and ESG data for SMEs) —** sell the tools to others. Examples: Circularise (Netherlands), the data layer behind digital product passports; Plan A (Germany), software that answers a buyer's sustainability questionnaire.

> *None of these companies describes itself as a "recycling company". Each changed who owns the product and for how long it stays in use — not simply what happens to it at the end of its life.*

3.2 Case Studies

Vinted — Vilnius, Lithuania, founded 2008 as a way to swap clothes with friends. In 2025: €1.1 billion revenue, €10.8 billion in goods sold on the platform (GMV), €62 million net profit. Lithuania has 2.9 million people, a market size comparable to Albania's — Vinted's scale came from access to the EU single market, not the home market. The model is circular by construction: every sale extends a garment's life, with no factory, no inventory, and no "green" claim required. As a sharing-platform model, the startup owns the trust and the logistics, not the goods.

Swapfiets (Netherlands, 2014) a bike subscription: the customer pays monthly, the company owns, repairs and swaps the bike. 266,000+ members across 45 cities in 8 countries; €91 million revenue in 2024, cash-flow positive. The asset never leaves the company's loop — parts are reused, frames refurbished. The incentive flips: a bike that breaks costs the company, not the customer.

Fairphone (Netherlands, 2013) a modular smartphone whose screen, battery and camera the user can replace with a screwdriver. Spare parts are sold for years, with long software support, fairly sourced materials and a transparent supply chain. It is, in effect, the phone that EU ecodesign and repairability rules were written for — designing for repair today is compliance tomorrow (see Gate 4, Section 4.3).

3.3 Why Bother: Four Kinds of Return

Circularity is a cost strategy and a sales strategy before it is an ethics strategy.

- **Cost and resilience —** less virgin material, less waste to pay for, less exposure to commodity and energy price shocks.
- **Consumer pull —** 35% of consumers would choose the better-for-environment product over a slightly cheaper one; 29% have dropped a brand over sustainability concerns.
- **Buyer and investor pull —** EU corporates now screen suppliers for it, and green finance lines price it in (see Gate 3, Section 4.3, and the funding instruments in Section 4.5).
- **Regulatory readiness —** every 2026 rule covered in Section 4 is cheaper to meet if the product was circular by design from the start.

3.4 How to Start: A Five-Step Roadmap

- **Validate the green idea —** problem, customer, willingness to pay, before the sustainability story.
- **Define a sustainable value proposition —** what is better for the customer and for the planet, in one sentence.
- **Design the circular business model —** use Sustainable Business Model Canvas to decide which of the four models in Section 3.1 fits, and who owns what.
- **Build supply chain and partners —** eco-materials, local sourcing, take-back partners, certifications.
- **Measure and tell —** KPIs, impact metrics, honest marketing, reporting.

3.5 Reference Guide

The session is built around the "Guide to Circular and Green Economy for Startups" (EU4Innovation · Entrepreneur Journey, 2024) — 106 pages, free, co-funded by the EU, BMZ and Sida, implemented with GIZ, the National Youth Congress and CIT. Its eight chapters cover: (1) understanding the circular economy, (2) green business ideation, (3) sustainable business models and the canvas, (4) sustainable supply chains, (5) financing sustainability — including Albanian resources, (6) legal requirements, certifications and standards, (7) marketing and branding, and (8) measuring impact and reporting.

4. The 2026 Update: Four Gates to the EU Market

4.1 What Changed Since the Guide Was Written

Every date below is real, and most of them are already behind us:

- 2024 — reference guide published.
- 1 January 2026 — CBAM (Carbon Border Adjustment Mechanism) enters its definitive regime.
- February 2026 — Omnibus I adopted: CSRD and CSDDD reporting narrowed to the largest firms.
- 12 August 2026 — PPWR (new EU packaging rules) applies.
- 27 September 2026 — EmpCo Directive applies (green-claims ban).
- 2026–27 — ESPR delegated acts roll out by sector (steel 2026; textiles and tyres 2027), introducing product passports.

At home, Albania's EPR Law No. 74/2025, adopted in late 2025 to align with the EU Waste Framework Directive, covers packaging, electronics, batteries, vehicles and used oils — the same logic as the EU's, on the Albanian side of the border.

4.2 You Are Not Regulated. You Are Screened.

After Omnibus I, EU sustainability-reporting law reaches only the largest companies: CSRD applies to firms with 1,000+ employees and €450 million+ turnover (reporting from FY2027); CSDDD (supply-chain due diligence) applies to firms with 5,000+ employees and €1.5 billion+ turnover (from July 2029).

Almost no Albanian startup is directly in scope of these two laws. But almost everyone is inside someone's value chain. The EU requirement therefore does not arrive as a law with a startup's name on it — it arrives through four other doors: what a company may say, what it may pack its product in, what its buyer asks it, and what it costs to cross the border. These are the four gates below.

4.3 The Four Gates

Each gate has a date, a rule, and one action to take.

Gate 1 — SAY: what you are allowed to claim

Instrument: the Empowering Consumers for the Green Transition Directive (EU 2024/825, "EmpCo"). No SME exemption; applies from 27 September 2026 to anyone selling to EU consumers, whether EU-based or not.

Banned from 27 September: generic claims such as "eco-friendly", "green", "natural" or "sustainable" unless proven with recognised excellent performance; "climate neutral" / "CO_2 neutral" claims based on offsets outside the company's own value chain; home-made sustainability labels or badges without a certified third-party scheme; and vague future pledges (e.g. "net zero by 2040") without a public, verified plan.

> *This already happens in court: in KLM (Amsterdam District Court, 20 March 2024), 15 of 19 advertising statements — including "CO2ZERO" and "more sustainable" — were ruled misleading under existing unfair-practices law. The separate Green Claims Directive was withdrawn in 2025; that is not a reprieve, since EmpCo is the instrument that applies. Example rebuild: "Eco-friendly packaging" → "Box made from 80% recycled cardboard, FSC Recycled certified. Recyclable with paper."*

Gate 2 — PACK: what you may put in

EU side: the Packaging and Packaging Waste Regulation (EU 2025/40, "PPWR"), a regulation and therefore identical across all 27 member states, applying from 12 August 2026. It requires all packaging to be designed for recycling (graded by 2030), minimised (no oversized boxes, e-commerce empty-space limits), to meet recycled-content targets for plastic packaging, to carry harmonised sorting labels, and restricts some single-use formats. Non-EU producers must register in each member state where they sell, via an authorised representative.

Albanian side: EPR Law No. 74/2025, adopted late 2025, transposing the EU Waste Framework Directive (2008/98/EC). It covers packaging, electrical and electronic equipment, batteries, vehicles and used oils. Producers and importers must register, report volumes, and pay a fee per tonne through a producer-responsibility organisation. Obligations are lighter for small producers, but registration is not optional — the logic mirrors the EU scheme: design once, comply twice.

> *Businesses built on this gate: Sulapac (Finland) sells a wood-based, microplastic-free material to brands replacing plastic; RePack (Finland) rents reusable e-commerce packaging that customers post back. Neither sells "green" — both sell a compliance problem, solved.*

Gate 3 — ANSWER: what your buyer will ask

Context: Omnibus I, February 2026. The law lands on the large EU customer; the questionnaire lands on its supplier. A typical questionnaire asks for a code of conduct, an EcoVadis rating, ISO 14001 certification, a carbon footprint, and waste and water data.

Protection: Omnibus I introduced a value-chain cap — an in-scope company may not demand more from a supplier with under 1,000 employees than the voluntary SME standard (VSME). This is a ceiling, not a floor, and is worth knowing by name.

Preparation: a two-page "VSME-lite" document covering energy use and an emissions estimate (Scope 1–2), waste/water/materials in and out, one paragraph each on environmental, labour and anti-corruption policy, and any certifications held or in progress.

> *This is also a business opportunity: providers such as Plan A and Coolset build software that answers exactly these questionnaires on behalf of smaller suppliers.*

Gate 4 — CROSS: what it costs at the border

CBAM (Carbon Border Adjustment Mechanism): in its definitive regime since 1 January 2026, covering iron and steel, aluminium, cement, fertilisers, electricity and hydrogen. The EU importer pays per tonne of embedded CO_2 and needs the exporter's emissions data to do so. A 50-tonne/year de minimis exemption applies per importer, but buyers request the data regardless.

ESPR (ecodesign and product passports): delegated acts apply by sector — iron and steel from 2026, textiles and tyres from 2027, furniture and aluminium from 2028. It introduces the Digital Product Passport (materials, origin, repairability, recycled content, scannable on the product), repairability scores, minimum durability rules, and a ban on destroying unsold goods. Albania's apparel and footwear contract-manufacturing (façon) sector is among the first in line.

> *Businesses built on this gate: Circularise (Netherlands) builds the traceability layer behind product passports; Fairphone (Section 3.2) is what a passport-ready product looks like. Any company that makes physical goods will soon need this data — or a supplier who already has it.*

4.4 The Four Gates at a Glance

This summary table is worth keeping on hand as a quick reference.

Gate	Instrument	Applies from	Who it reaches	Immediate action
1 · SAY	EmpCo Directive (EU 2024/825)	27 Sep 2026	Anyone selling to EU consumers	Substantiate or delete every generic green word
2 · PACK	PPWR (EU 2025/40) + Albanian EPR Law 74/2025	12 Aug 2026	Anyone putting packaged goods on the market	Check packaging design; register with a producer-responsibility organization
3 · ANSWER	Omnibus I (CSRD / CSDDD)	Feb 2026	Suppliers to larger EU firms	Write a two-page VSME-lite; know the value-chain cap
4 · CROSS	CBAM · ESPR / product passports	1 Jan 2026 · 2027+	Metals, materials, textiles, footwear, furniture	Start collecting product-level energy & material data

4.5 Funding and Support Instruments

Green compliance is the ticket to the funding lines below, not simply a cost on top of them:

- **EU Growth Plan / Reform and Growth Facility —** €6 billion for the Western Balkans, 2024–27, paid against reforms; Albania's tranches include competitiveness and innovation reforms.
- **IPARD III —** EU rural-development grants for agro-processing and food, where circular packaging, energy efficiency and waste valorisation score well.
- **EBRD Green Economy Financing Facility (GEFF) —** green credit lines through local Albanian banks for energy efficiency, renewables and resource-efficient equipment, open to SMEs, not only corporates.
- **Horizon Europe / European Innovation Council (EIC) —** Albania is an associated country, eligible for research, innovation calls and EIC funding on the same terms as EU member states.
- **EU4Innovation Challenge Fund and other Albanian ecosystem instruments —** listed with contacts in Chapter 5 of the reference guide.

5. Green Claim Clinic: Readiness Tools

5.1 Monday Morning: Three Actions

- **Before 27 September —** read every green word on your product, packaging, website and social media. Substantiate it with a number and a source or delete it.
- **This month —** hold your packaging against the PPWR checklist and register your business under EPR Law 74/2025 before the fee becomes a fine.
- **This quarter —** write the two-page VSME-lite, so the first EU buyer who asks receives it in an hour instead of a month.

5.2 EU Readiness Self-Assessment Card

Work in pairs. Answer yes or no to each statement below, then count the total number of "yes" answers.

- We use "eco / green / natural / sustainable / climate-neutral" on any product, label, website or post.
- We have a number and a source for every environmental claim we make.
- Our packaging is a single, recyclable material, or we know why it is not.
- We are registered (or know how to register) under EPR Law 74/2025.
- An EU customer has ever sent us a questionnaire, code of conduct or ESG request.
- We could send energy, waste and emissions figures for last year within a week.
- We make or sell goods with steel, aluminium, cement, textiles, footwear or furniture.
- We know the origin and material composition of our main product.
- We sell or plan to sell to EU customers within 24 months.
- Someone in the team owns "EU compliance" by name.

Your score band indicates which gate to start with:

Score	Band	What it means / where to start
0–3	**Not yet exposed**	The EU is not asking you anything yet. Build good habits now, while they cost nothing: honest claims, clean packaging, one page of data. Start with the guide, chapters 3 and 6.
4–7	**Exposed through your buyer**	You are already in an EU value chain, or about to be. The questionnaire is coming before the law is. Start with Gate 3 — write the two-page VSME-lite this quarter.
8–10	**Directly exposed**	You sell to EU consumers or make goods in the passport sector. Two deadlines are already behind you, and one is only weeks away. Start with Gates 1 and 2 — claims and packaging, this month.

5.3 Worked Examples: Rebuilding Real Green Claims

The pattern is the same each time: remove the adjective, add the number, the source and the place.

Product	The claim today	Which gate it fails, and why	Rebuilt claim (survives 27 Sep)
Olive oil	"BIO olive oil — 100% natural"	Gate 1 — "Bio"/"organic" is a protected term under EU Regulation 2018/848: without certification it is illegal, not just	"Extra virgin olive oil, cold-pressed within 24h of harvest, acidity 0.3%. Groves in Berat. Certified

Product	The claim today	Which gate it fails, and why	Rebuilt claim (survives 27 Sep)
		vague. "Natural" is a generic claim with no proof.	organic — control body code on the label" (or drop 'bio' until certified).
Honey / jar	"Natural honey, environmentally friendly packaging"	Gates 1 + 2 — "environmentally friendly packaging" is exactly the generic claim the directive names; the jar must meet PPWR recyclability and be registered under Law 74/2025.	"Raw honey, unheated and unfiltered, from 40 hives above Gjirokastër. Glass jar, fully recyclable — return it to any stockist for 30 lek off the next one."
T-shirt	"Sustainable clothing, climate neutral"	Gates 1 + 4 — "sustainable" is generic; "climate neutral" via offsets is banned outright; textiles get a product passport from 2027.	"100% GOTS-certified organic cotton, sewn in Shkodër. 2.1 kg CO_2e per shirt, measured, not offset. Free repair for two years."

6. Key Takeaways

- The rules have dates, not opinions — most of the 2026 deadlines are already behind us or only weeks away.
- Circularity is a business-model choice, a cost strategy and a compliance shortcut, not only an ethics statement.
- Which gate to walk through first is a business decision — but doing nothing is no longer a viable option after 27 September 2026.

PART II — GDPR: Law No. 124/2024

Personal data protection in the age of AI — a practical focus for startups and technology professionals

1. Introduction: Why This Topic Matters Now

Nearly every sector of the economy and society now uses personal data in increasingly numerous and complex ways. A startup with only five employees can process the data of 100,000 users — company size does not reduce, or replace, responsibility for data protection.

The growth of AI has changed how data is collected, analysed and used: data can train AI systems, analyse user behaviour, build profiles, and even feed automated decisions. At the same time, the use of online services, SaaS platforms and cloud technologies means personal data no longer necessarily stays within one system or one company — it can be processed by different service providers for storage, analysis, management or transmission.

Sectors such as finance, insurance, health and education are increasingly using data analytics and automated systems to assess risk, offer personalised services, or support decision-making. As a result, privacy risk today is no longer only about a traditional database holding names, addresses or phone numbers. Risk can appear in the algorithm analysing the data, in the app collecting it, in the cloud platform storing it, in a camera or sensor gathering information, in a platform profiling users, or in an automated system whose decision directly affects an individual.

> *Compliance with data-protection requirements cannot be addressed at the end of a project, once the technology is already built. It must be considered from the design and development stage (Article 23 of the Law).*

2. The New Albanian Legal Framework

- Law No. 124/2024 "On the Protection of Personal Data" entered into force on 1 February 2025 and repeals Law No. 9887/2008.
- It is fully aligned with the GDPR and with Directive (EU) 2016/680 on processing by competent authorities (the "Police Directive").
- A key shift is the philosophy of accountability: it is no longer enough to say, "we have a privacy policy." An organisation must be able to show why its processing is lawful, what risk it assessed, what measures it took, and how this is documented.
- The framework is accompanied by 10 secondary/implementing acts and by guidance and practice from the Commissioner's office — it should be read as a system, not only as a legal text.

3. From "Do We Have a Privacy Policy?" to "Can We Prove Compliance?"

This is arguably the most important shift to take from this session. The traditional question was: do we have the documentation? The new question is: can we prove compliance?

In practice this means an organisation should be able to say, at any time:

- What data it holds.
- Why it processes that data, and on what legal basis.
- Who has access to it.
- How long it is kept.
- Where it is transferred.
- What risk this creates.

- What measures have been taken to address that risk.

> *Article 22 addresses the controller's accountability, while Article 27 addresses records of processing activities. Documentation is not an administrative add-on, it is part of the compliance mechanism itself.*

4. Core Principles Governing Any Data-Processing Project

These principles (Article 6 and related controller obligations) should be on the table whenever a new process is designed:

- **Lawfulness, fairness and transparency** - the individual must understand what is happening to their data.
- **Purpose limitation** - data collected for one purpose is not automatically reused for another.
- **Data minimisation** - the question is not "what could we collect?" but "what do we actually need?"
- **Accuracy and storage limitation** - data must be accurate and kept no longer than necessary.
- **Security** - confidentiality, integrity and availability, proportionate to the risk.
- **Accountability** - the organisation must be able to demonstrate compliance, not merely assert it.

5. Controller, Processor or Sub-Processor? The First Question for Any SaaS

For SaaS companies in particular, this is a foundational question: who decides the purpose and the means of processing?

- **Controller** - determines the purposes and means of processing; the startup decides why and how data is used.
- **Processor** - processes data on the controller's behalf, following instructions — typically the SaaS or cloud provider.
- **Sub-processor** - third parties further down the chain: hosting, analytics, other SaaS tools.

When a startup selects a cloud provider, CRM, analytics platform, email provider or AI service, it needs to map its entire processing chain before signing. Responsibility for the data does not disappear simply because it has been placed in the cloud.

6. Territorial Scope

The law applies to the processing of personal data when:

- The controller or processor is established in the Republic of Albania, regardless of whether the processing itself takes place in Albania or abroad; or
- The controller or processor is established outside Albania, but the processing relates to data subjects located in Albania, in connection with offering them goods or services, or with monitoring their behaviour, to the extent that behaviour takes place in Albania; or
- The controller or processor is established in a territory where Albanian law applies under public international law.

> *In the second case above, a non-Albanian entity must, in principle, appoint a representative established in Albania, subject to the exceptions set out in the law. The Commissioner may investigate, order measures and impose sanctions; enforcement outside Albanian territory requires cross-border mechanisms.*

7. Privacy by Design and by Default

Privacy by Design is one of the concepts where the law meets software development directly. Introducing privacy only at the end, once a system is already built, makes any change far more costly. Three stages are useful to keep in mind:

- **Plan** - purpose, minimal data needed, risk, roles, retention period.
- **Build** - pseudonymisation, encryption, access control, logging, deletion.
- **Default** - the system's initial configuration should be as protective as possible — the user should not have to switch off dozens of options to gain privacy; less data, less access, less retention by default.

> *The "golden question" for a developer: what is the minimum data I actually need for this feature?*

8. Profiling and Automated Decision-Making

Consider three illustrative sectors: a bank using AI for credit or risk scoring; an insurer using an algorithm for risk assessment or pricing; a recruitment company using AI to rank CVs. In each case, the question is whether profiling is taking place and whether the resulting decision produces significant effects on an individual.

"The algorithm decided" is not a legal answer. Where a decision is based solely on automated processing and produces such effects, the law requires transparency, safeguards and, where required, the possibility of human intervention and the right to contest the decision. This is especially relevant in finance, insurance, HR, education and healthcare.

9. Data Protection Impact Assessment (DPIA)

Not every technology project automatically requires a DPIA. But where processing, especially involving new technologies, may create high risk to individuals' rights and freedoms, an impact assessment must be carried out.

Typical trigger scenarios include use of new technology, profiling with significant consequences, large-scale processing of sensitive data, and systematic monitoring of public spaces.

A DPIA must analyse the purposes of processing, the necessity and proportionality of the processing, the risks it creates, and the measures and safeguards that mitigate them. It is a decision-making process, not simply a document for the file.

> *Articles 31 and 32 place this obligation on the controller. Where high risk remains even after mitigation measures, prior consultation with the Commissioner is required before processing begins; for certain processing carried out in the public interest, prior consultation and authorisation may also be required by law. The obligation of prior consultation enters into force in February 2027.*

10. Cybersecurity Is Not the Same as Data Protection

A system can be technically very secure and still have a data-protection problem.

- **Cybersecurity asks:** "Is the system protected from unauthorized access?" — encryption, access control, backup, testing, monitoring, recovery.
- **Data protection asks, in addition:** "Do we have the right to process this data? Do we need it? Are we using it for the right purpose? Are we keeping it for the right length of time?"

> *In the event of a personal data breach, Article 29 requires notification to the Commissioner as soon as possible and, where required, no later than 72 hours after the controller becomes aware of it. Breach response must therefore be both technical and legal.*

11. Cloud, SaaS and International Transfers

For a startup, data often passes through several systems: the customer relates to the controller; the SaaS provider acts as processor; sub-processors — cloud hosting, analytics — sit further down the chain.

Before signing with any vendor, a company should:

- Identify all recipients of the data and clarify the controller / processor / sub-processor roles across the chain.
- Check the countries in which the data will be processed.
- Verify the protective measures in place and whether an adequacy decision covers the destination country; if not, appropriate safeguards (such as standard contractual clauses) are required.

> *Practical rule: before signing a contract, it is not enough to look at price and the Service Level Agreement. Data-protection terms, the location of processing, and the sub-processor chain must be reviewed as well.*

12. The Data Protection Officer (DPO): A Compliance Function, Not a Formal Title

A DPO is required for: public authorities; regular and systematic monitoring of individuals on a large scale; and large-scale processing of special-category or criminal-record data (Articles 33–34).

The DPO advises, monitors compliance, trains staff, participates in DPIAs, and cooperates with the Commissioner.

> *In a small startup without a dedicated DPO, responsibilities are often distributed across founders/management, legal/privacy, product and engineering. Final accountability for compliance always rests with the organisation's management, or the controller — not only with whomever handles privacy day to day. Especially for AI, cloud and analytics, privacy governance must be an ongoing process, not a document produced once and forgotten.*

13. Sanctions: The Risk Is Not Only Reputational

- Article 93 requires that any sanction be effective, proportionate and dissuasive.
- Article 94(1): fines of up to 1 billion lekë, or 2% of total annual global turnover, for the relevant categories of infringement.
- Article 94(2): fines of up to 2 billion lekë, or 4% of total annual global turnover, for more serious infringements, subject to the conditions of the law.

> *These are legal ceilings, not automatic fines. The methodology adopted by the Commissioner in 2025 calculates the sanction in steps: identifying the processing, a starting point, aggravating or mitigating circumstances, the legal ceiling, and then a check of effectiveness, proportionality and dissuasiveness. The size of a fine cannot be read outside the circumstances of the specific case.*

14. Action Checklist for Startups and Companies

14.1 Organization and Lawfulness

- Specify the data held and define the purposes of processing.
- Apply a valid legal basis to every processing activity.
- Respect data minimization.
- Inform data subjects (Article 13).
- Where consent is the legal basis, obtain valid consent under Articles 7(1)(a), 8 and 9.

> *If a company cannot prove compliance, the problem is not only technical.*

14.2 Internal Rules and Responsibilities

- Draft internal regulations for data processing (Article 28).
- Have employees or collaborators with data access sign confidentiality declarations (Article 30).
- Document processing activities and maintain the Record of Processing Activities (Article 27).
- Appoint a Data Protection Officer where required (Articles 33–34).

14.3 Security and Risk Management

- Carry out a DPIA where needed and, where required, a prior consultation (Article 31 — in force from February 2027).
- Implement appropriate technical and organisational security measures.
- Review cloud usage and international transfers.
- In the event of a breach, notify the Commissioner within 72 hours.
- Prepare and apply Codes of Conduct where relevant (Article 35 — in force from February 2027).

> *Overarching logic: Law 124/2024 → Accountability → Privacy by Design → Risk-based compliance.*

15. Key Takeaways

- Data protection should not be seen as an obstacle to innovation — for new technologies, it is part of product quality.
- A powerful AI system that is not transparent, proportionate and secure creates risk. A SaaS that works technically but does not know where customer data goes creates risk. A system that collects more data than it needs creates risk.
- The objective is not only "being compliant with the law" — it is building trustworthy technology in which privacy is part of the architecture.
- Privacy builds trust. Trust enables innovation.

PART III — AI and Cybersecurity Standards

Workshop Session II: what startups need to know for the EU market

1. Session Overview

This session covers three areas, each ending with a short set of concrete actions:

- **AI Compliance and Ethics —** the EU AI Act's risk-based rules and what they mean for your product.
- **Cybersecurity Readiness —** the standards and controls EU partners and regulators expect to see.
- **Digital Single Market Standards —** data flows, eIDAS trust services and cross-border design — relevant even while a company is still purely local.

2. The Stakes: The Clock Is Already Running

A company can be local this year and still fall into scope the moment it touches an EU user, an EU model provider, or a regulated buyer.

- **GDPR / Law 124/2024 —** no small-startup exemption. Applies from a company's very first EU user, regardless of size or funding stage.
- **DORA (Digital Operational Resilience Act)** conditional, ICT third-party exposure. Binds a company only if it sells into a financial entity — and then arrives as a contractual control package, not as a choice.
- **EU AI Act —** literacy obligations now, high-risk obligations later. Articles 5 (prohibited practices) and 4 (AI literacy) already apply. Transparency (Article 50) applies from August 2026. Annex III high-risk duties apply from 2 December 2027, following the AI Omnibus.
- **Cyber Resilience Act (CRA) —** a product rule, not a policy. If a company places software or a connected product on the EU market, secure-by-design and vulnerability-handling obligations apply, in full application from 11 December 2027.

> *For a company under two years old, the design decision taken now is cheaper than a retrofit forced by the first EU diligence request.*

3. Part 1 — AI Compliance and Ethics

How the EU AI Act shapes what a company can build, and how it must build it.

3.1 The EU AI Act: A Risk-Based Framework

In force since 1 August 2024. There is no SME exemption on classification. The AI Omnibus (in force July 2026) moved some high-risk dates but did not lower the substantive bar. The Act sets four risk tiers:

- **Unacceptable risk —** banned outright, e.g. social scoring, manipulative or exploitative AI systems.
- **High risk —** Annex III / Annex I obligations: risk management, data governance, logging, human oversight, technical file. Key dates: 2 December 2027 (Annex III) and 2 August 2028 (Annex I).

- **Limited risk —** transparency duties, e.g. disclosing that users are interacting with an AI system.
- **Minimal risk —** most product features sit here; GDPR/Law 124/2024 and sector law still apply, but the AI Act adds no extra layer.

> *Live obligations timeline: Article 5 prohibitions and Article 4 literacy (from February 2025) GPAI (general-purpose AI) model duties (from August 2025) · Article 50 transparency (from August 2026) · Annex III high-risk duties (from 2 December 2027).*

3.2 AI Act at Founding Stage: Provider vs Deployer

- **Decide your role first —** "provider" if placing a system on the market or under your own name; "deployer" if using a third-party model in production.
- **Classify before you scale the feature —** likely Annex III (high-risk) candidates include education scoring, health triage, credit-like decisions, recruitment, and biometric identification.
- **Human oversight where the output binds —** required for high-risk systems, and still rational for any decision that changes a person's access to money, care or identity.
- **Training and vendor data —** document the source, the lawful basis, the retention period, and whether personal data left Albania or the EEA. Bias testing is a control, not a slide.
- **Technical file, proportionate —** architecture, intended purpose, known limits, evaluation. SMEs get simplified documentation — not an empty file.
- **Literacy is already due —** Article 4 applies to staff who build or operate AI, including founders using tools such as Copilot or a third-party model on customer data.

3.3 Part 1 — Decisions for This Month

- Write a one-page intended-purpose and risk-tier note. If medium to high risk, treat 2027 as a build deadline, not a distant date.
- If users interact with a model or see synthetic content, transparency obligations are a product requirement from August 2026.
- Keep an AI inventory: system, role (provider/deployer), data classes, vendor, location of processing.
- Name an accountable owner. In a five-person team that is a founder, not a future hire.
- Do not wait for a purely domestic law before starting classification — extra-territorial application already runs on EU users and EU market placement.

4. Part 2 — Cybersecurity Readiness

The controls and certifications EU partners and regulators expect to see.

4.1 Minimum Control Set Before First Diligence

- Asset and data inventory: know what you have and where it lives.
- Robust infrastructure; secure coding; threat modelling.
- A written incident-response plan, with defined roles, a 72-hour notification path, tested at least once a year.
- Access control, encryption and secure development practices.
- Third-party and vendor risk assessed before onboarding.
- Ongoing employee security-awareness training.
- An external review scheduled before the first EU or regulated-buyer questionnaire arrives.

4.2 What Security Reviews Most Often Find

- No multi-factor authentication on admin, cloud or email accounts — the single easiest win most teams still skip.
- API keys and passwords stored in code repositories, chat messages or shared documents.
- One shared login used by the whole team instead of individual, traceable accounts.
- AI tools and vendors given far more data access than the task actually requires, including personal data.
- No one, not even part-time, owns security until something goes wrong.

> *The encouraging news: every one of these gaps is fixable in a week, not a year.*

5. Part 3 — Digital Single Market Standards

What it takes to move data, services and trust seamlessly across EU borders.

5.1 Practical Requirements

- **Free flow of data and services —** products should be designed so data and services move freely across EU member states.
- **Digital identity and trust services (eIDAS) —** if a company signs contracts, onboards users or verifies identity, it needs a qualified trust service. A home-grown "e-signature" will not satisfy EU counterparties.
- **Interoperability by design —** systems built on open, common standards integrate faster with EU platforms, banks and public administrations.
- **Consumer and platform rules —** transparency and accountability obligations shaped by the Digital Services Act and Digital Markets Act.

5.2 Cross-Border Before You Are Cross-Border: Action Checklist

- Map every data flow now: where it is collected, stored, inferred, and which vendor holds a copy.
- Use eIDAS-qualified signature and identity providers if you close contracts or run onboarding remotely.
- Expect accession alignment to import more of the EU acquis over time — design to the EU text; local rules are converging, not diverging, from it.
- Use tools such as DiVA or the local EDIH (European Digital Innovation Hub) network for a digital-maturity assessment.
- Remember that a local-only customer base today does not freeze GDPR extra-territorial reach, or CRA applicability, if the product is later placed on the EU market.

6. Roadmap: Before Entering EU Markets

- 1. Map applicable rules to your product (Law 124/2024, EU AI Act, NIS2, DORA, sector-specific rules).
- 2. Appoint an accountable owner — a CISO, DPO or compliance lead.
- 3. Build the technical and organisational controls the mapping requires.
- 4. Document everything — policies, DPIAs, risk registers, records of processing.
- 5. Test, audit and certify — e.g. ISO 27001, external assessment.
- 6. Monitor, update and re-assess as the product and the rules evolve.

7. Maturity Path: What to Do Before Year Two

Most startups are pre-scale; the third stage below is a target state to design toward, not a description of where most teams are today.

Stage	Core controls in place	Add when relevant
MVP / still local	Secure SDLC, data minimisation, lawful basis, vendor DPAs, MFA on admin paths	Intended-purpose note if any model touches users or their data
First revenue / first EU customer	External review; evidence pack (policies, logs, DPIA/AIIA where triggered)	Transfer tool if any processor sits outside the EEA
First regulated or EU buyer	Named compliance owner; core registers in place (Record of Processing Activities); breach path; AI inventory	DORA-specific pack, only if the buyer is a financial-services entity

8. Discussion Questions

- Provider or deployer — has this been documented for every model used in the product?
- If a company laptop disappeared tonight, what is the response plan?
- Which control would fail first in an EU buyer's due-diligence questionnaire?

9. Key Takeaways

- Extra-territorial rules (GDPR/Law 124/2024, EU AI Act, CRA) can apply before a company sells its first unit abroad.
- Design decisions taken now — on data minimisation, access control, documentation and AI classification — are cheaper than retrofits demanded later by an EU diligence process.
- Security and compliance readiness are incremental and buildable within weeks; the roadmap above turns broad regulatory categories into a sequence of concrete, ownable actions.