Become Busy Xelerator

TechX – Digital Innovation & Technology

PRESENTATION 3

CYBERSECURITY & DATA PROTECTION

Start Slide

Project number: 2023-1-EL02-KA220-YOU-000160907

www.becomebusy.eu www.fifty-fifty.gr

01.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the Youth and Lifelong Learning Foundation (INEDIVIM). Neither the European Union nor the granting authority can be held responsible for them.

INTRODUCTION

CYBERSECURITY & DATA PROTECTION FOR ENTREPRENEURS

Cybersecurity and data protection are not just IT concerns; they are business fundamentals that shape user trust, brand reputation, and regulatory risk. For early-stage teams, a few disciplined practices can prevent costly incidents and keep growth on track. This session connects the legal "why" with the technical "how," showing practical steps to safeguard your startup and your users from day one.

- Focus: GDPR & legal bases, core security controls, ethical data use
- Payoff: reduced risk, smoother sales, partner confidence
- Mindset: "secure by default, private by design"
- Note: this is guidance, not legal advice

TRUST AS A GROWTH STRATEGY

Customers buy confidence as much as features. Demonstrating security competence—clear policies, responsible data handling, rapid incident response—can unlock sales, especially with enterprise clients. Treat security as a product attribute you can design, measure, and improve.

- Signals: status page, audit logs, security page on site
- Artifacts: DPIA summaries, penetration test reports
- Proof: uptime SLAs, breach-response drills
- KPI: deal velocity ↑ when trust blockers ↓

THE BBX CONTEXT: BUILDING GOOD HABITS EARLY

In the BBX ecosystem, distributed teams handle user data across borders and tools. Establishing uniform privacy and security habits—classification, access control, encryption, and clear ownership—keeps collaboration safe and compliant, and it scales as projects mature into ventures.

- Practices: shared policies, least-privilege access, secure docs
- Tools: password manager, SSO/MFA, encrypted storage
- Reviews: onboarding/offboarding checklists
- Outcome: fewer leaks, faster audits

THREATS STARTUPS ACTUALLY FACE

Most startups are not targeted by nation-states; they are hit by opportunistic attacks: stolen credentials, phishing, misconfigured cloud buckets, vulnerable dependencies, or lost devices. Designing controls for these realistic threats gets you 80% of the protection at 20% of the cost.

- Top risks: credential stuffing, phishing, S3/GCS exposure, weak backups
- Vectors: third-party apps, public repos, test data in prod
- Counter: MFA, hardening, patching, backups, monitoring
- Rule: eliminate single points of failure

PRIVACY & SECURITY: DIFFERENT BUT INTERTWINED

Security protects data from unauthorized access; privacy governs how and why you collect, process, and share it. You need both: perfect security won't fix unlawful processing, and perfect privacy won't help if attackers can walk in. Align your privacy promises with your security architecture.

- Security ≠ Privacy: different controls, same goal—trust
- Align: data minimization → fewer assets to defend
- Document: processing map → security scope
- Audit: test promises against technical reality

GDPR & LEGAL FRAMEWORKS

GDPR IN ONE SLIDE

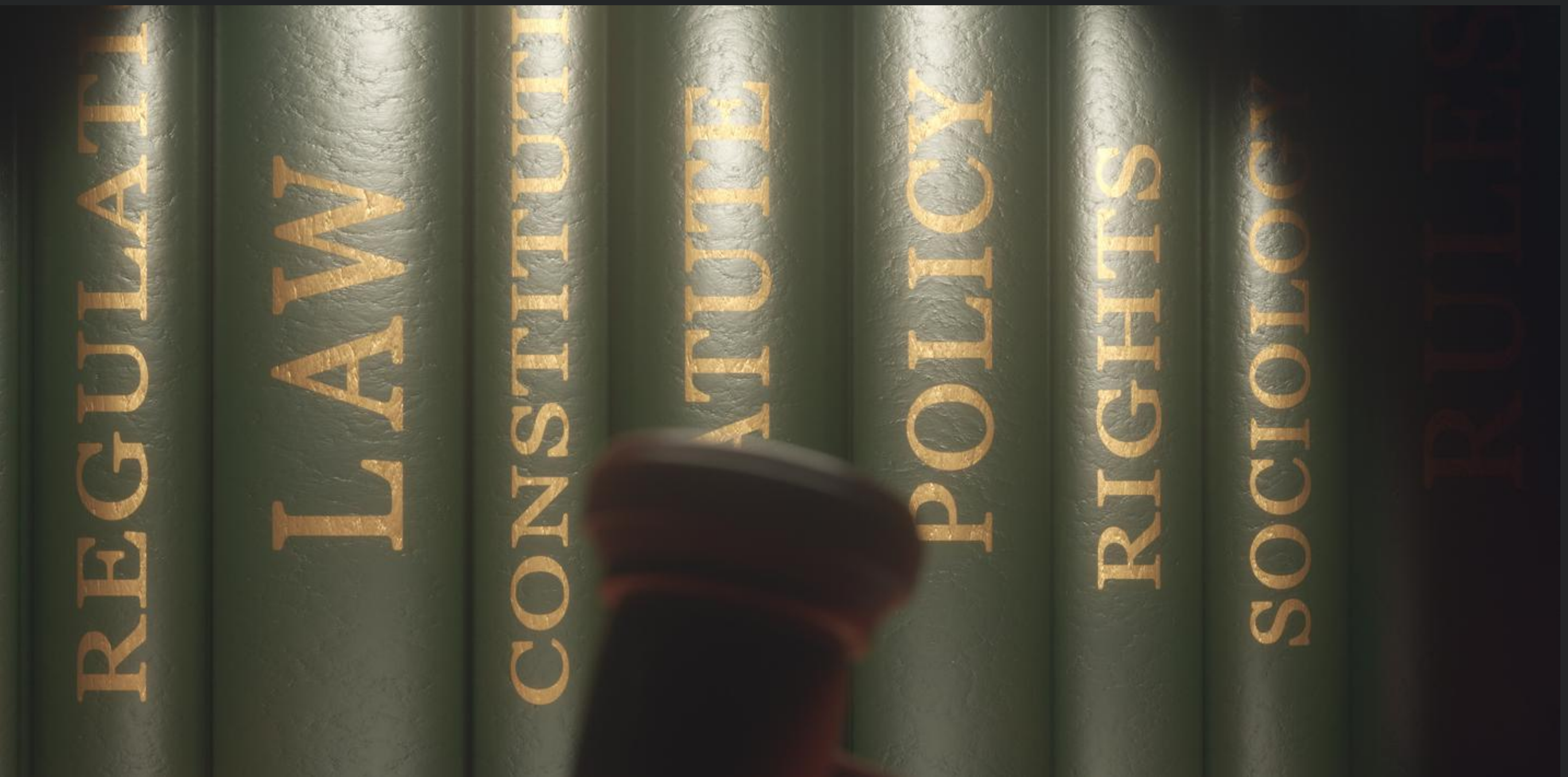
The GDPR centers on lawful, fair, and transparent processing of personal data. It grants people rights over their data and imposes duties on organizations that act as controllers or processors. For startups, GDPR discipline is also a sales enabler: many B2B deals require it.

- Core principles: purpose limitation, minimization, accuracy, storage limits, integrity/confidentiality, accountability
- Roles: controller vs. processor
- Scope: EU residents' personal data, wherever processed
- Culture: "say what you do, do what you say, prove it"

LAWFUL BASES FOR PROCESSING

Every processing activity needs a lawful basis. Common options are consent, contract necessity, legitimate interests (balanced), legal obligation, vital interests, and public task. Choose one per purpose and document your reasoning.

- B2C typical: consent, legitimate interests (with LIA)
- B2B typical: contract necessity for service delivery
- Don't stack bases; pick the most appropriate
- Keep records in your RoPA (record of processing activities)



DATA SUBJECT RIGHTS

People can access, rectify, erase, restrict, object, and port their data. Build simple processes to respond within statutory timelines and keep evidence of fulfillment. Rights-handling is both a UX moment and a compliance requirement.

- Provide: self-service portals or clear contact
- Timelines: respond without undue delay
- Verify identity before action
- Log requests and outcomes

PRIVACY BY DESIGN & DPIAS

Embed privacy into product decisions—collect less, anonymize where possible, set conservative defaults. For high-risk processing (e.g., large-scale sensitive data, systematic monitoring), conduct a Data Protection Impact Assessment to identify and mitigate risks.

- Triggers: new tech, profiling, sensitive categories
- Steps: describe processing → assess necessity → assess risks → mitigate
- Output: action plan and sign-offs
- Bonus: DPIA doubles as architecture review

PROCESSORS, DPAS & AGREEMENTS

If vendors process personal data for you, you must have a compliant Data Processing Agreement that sets instructions, security measures, subprocessor rules, and audit rights. Vendor risk management is a core GDPR control.

- Checklist: purpose, instructions, confidentiality, security, breach notice, deletion/return
- Due diligence: SOC 2/ISO 27001, pen test, policies
- Track subprocessors and locations
- Reassess annually or on material change

INTERNATIONAL TRANSFERS

Transferring personal data outside the EEA requires safeguards such as Standard Contractual Clauses and transfer risk assessments. Know where your data lives and ensure equivalent protection.

- Map: data residency by service
- Use: SCCs + technical measures (encryption, pseudonymization)
- Document: Transfer Impact Assessment
- Communicate clearly in privacy notices

BREACH NOTIFICATION BASICS

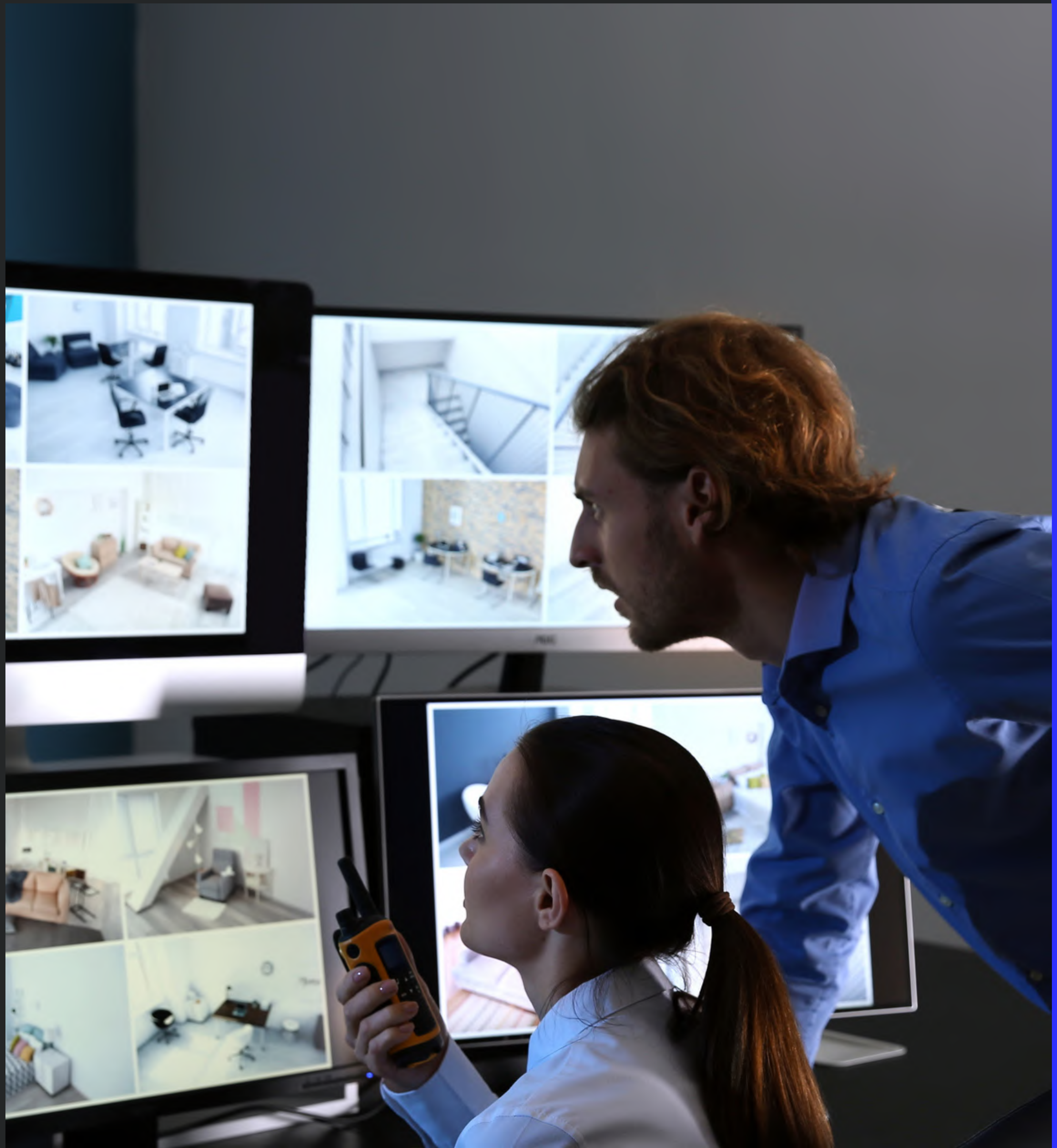
A personal data breach may require notifying the authority within 72 hours and, in some cases, affected individuals. Have a playbook: detect, contain, assess, decide, notify, learn.

- Define “breach” broadly (confidentiality, integrity, availability)
- Keep decision logs and timelines
- Template notices ready (regulator + users)
- After-action reviews to prevent recurrence

OTHER FRAMEWORKS & STANDARDS

Beyond GDPR, know the nearby landscape: ePrivacy rules for cookies/communications, security standards like ISO 27001 and SOC 2, and sectoral obligations. Use standards as roadmaps, not obstacles.

- Align with: NIST CSF, ISO 27001 Annex A controls
- Cookie consent & logs for ePrivacy compliance
- Map requirements to your product surface
- Prioritize controls with highest risk reduction



CYBERSECURITY BASICS FOR STARTUPS

SECURITY POSTURE IN 10 CONTROLS

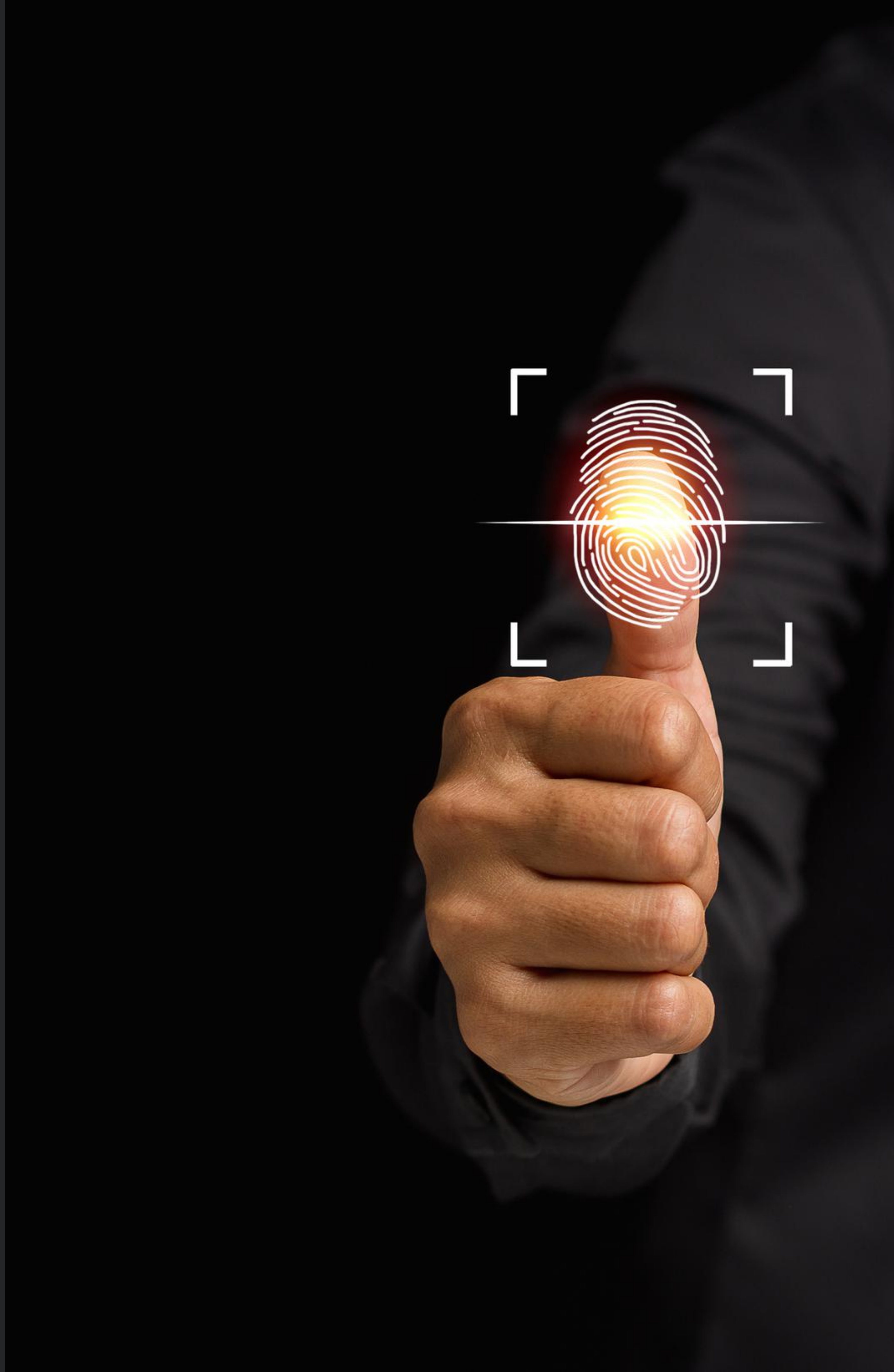
Startups can achieve strong baseline security with a concise set of controls covering identity, endpoints, infrastructure, and data. Aim for depth where it matters: identity proofing, MFA everywhere, reliable backups, and least privilege.

- Top 10: MFA, password manager, patching, EDR, backups (3-2-1), logging, access reviews, secrets management, vendor review, incident response plan
- Policy-lite: short, actionable, enforced
- Train: phishing drills + onboarding security

IDENTITY & ACCESS MANAGEMENT

Identity is the new perimeter. Centralize accounts, enforce MFA/SSO, and grant access on a least-privilege, need-to-know basis. Review access when roles change and remove stale accounts immediately.

- Tools: SSO with MFA, SCIM provisioning
- Enforce: device + user context (conditional access)
- Cadence: quarterly access reviews
- Beware: shared accounts and orphaned credentials



ENDPOINT & DEVICE SECURITY

Laptops and phones are common breach paths. Encrypt devices, enable remote wipe, and deploy endpoint detection and response. Separate personal and work contexts where possible.

- Controls: full-disk encryption, EDR/antivirus, auto-lock
- MDM: enforce policies, patch OS/apps
- BYOD: minimum standards or VDI/browser isolation
- Inventory: know every device, every time

SECURE DEVELOPMENT LIFECYCLE (SDL)

Bake security into coding: threat model new features, use secure defaults, scan dependencies, and run automated checks in CI/CD. Review critical code paths and never store secrets in repos.

- Tools: SAST/DAST/Dependency scanning
- Patterns: parameterized queries, output encoding, rate limits
- Secrets: vaults (not .env in repos)
- Ship: small changes, rapid rollbacks

APP SECURITY BASICS (OWASP-INSPIRED)

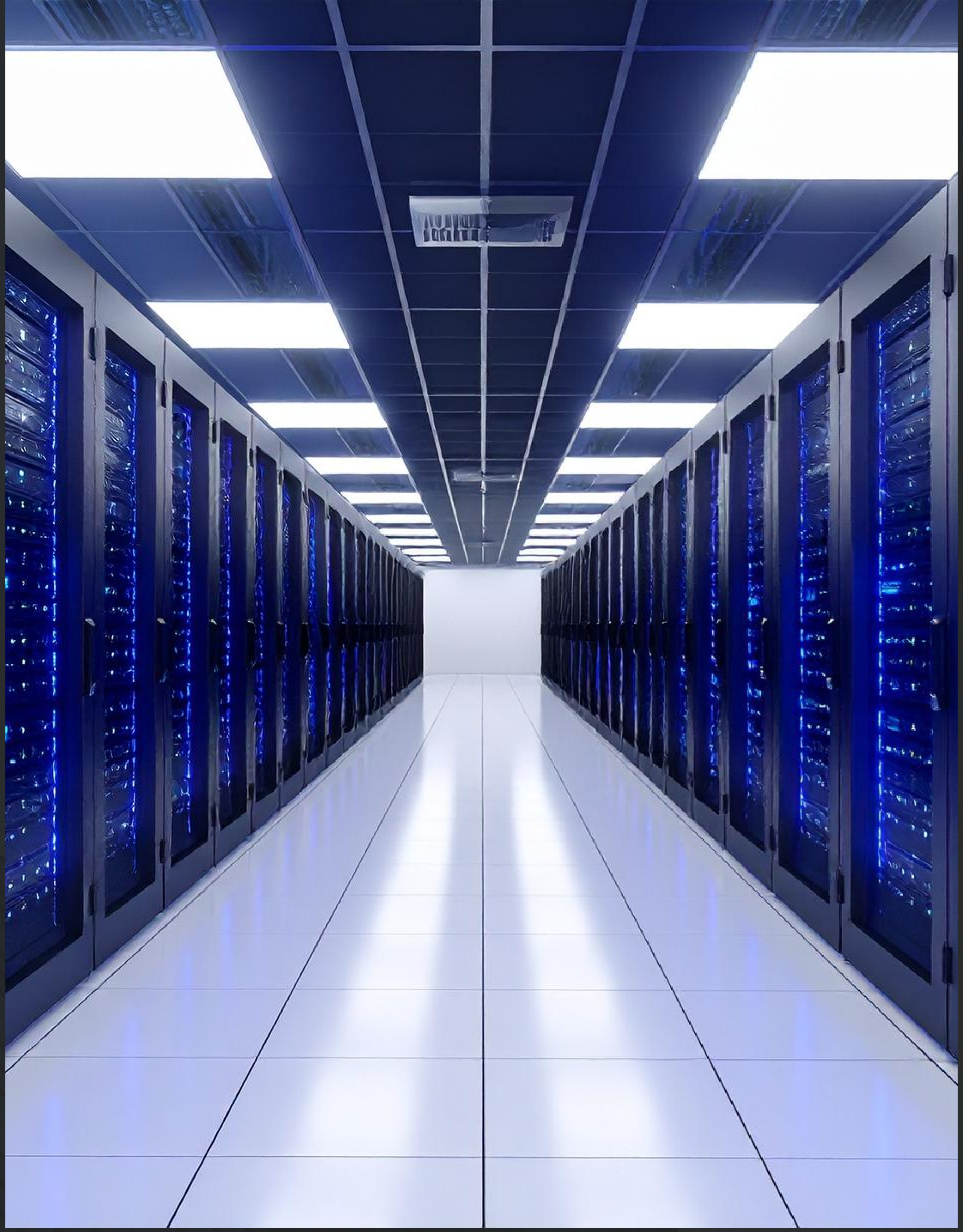
Prevent the common bugs: injection, broken auth, misconfigurations, sensitive data exposure, SSRF. Treat authentication, session management, and authorization as first-class features.

- Controls: MFA, secure cookies, CSRF protection
- Encrypt in transit (HTTPS) & at rest
- Validate input; sanitize output
- Principle: deny by default, allow minimal

CLOUD & INFRASTRUCTURE HYGIENE

Cloud is a shared responsibility. Configure IAM tightly, segment networks, lock down storage buckets, and automate baselines with infrastructure-as-code. Monitor drift and unusual activity.

- Guardrails: least-privilege roles, no public buckets
- IaC: reproducible, reviewed, versioned
- Monitoring: logs to a central sink + alerts
- Backups: tested restores, not just snapshots



DATA CLASSIFICATION & MINIMIZATION

Classify data (public, internal, confidential, sensitive) and tie controls to each class. Collect only what you need, store it where it belongs, and delete it when it's no longer required. Less data = less risk.

- Map: systems of record vs. analytics copies
- Retention: default time limits + deletion jobs
- Pseudonymize/anonymize for analysis
- Track lineage: where data flows and why

MONITORING, LOGGING & DETECTION

You cannot protect what you cannot see. Centralize logs from apps, endpoints, and cloud. Define detections for suspicious behavior and rehearse your response.

- Sources: auth logs, API gateways, EDR, WAF
- Detections: brute force, privilege escalation, data exfiltration
- Playbooks: who does what, in what order
- Test: tabletop exercises twice a year

INCIDENT RESPONSE ESSENTIALS

Incidents happen. A good response limits damage and speeds recovery. Establish roles, communications templates, and escalation paths before you need them.

- Stages: prepare → detect → contain → eradicate → recover → learn
- Channels: out-of-band comms for crisis
- Evidence: preserve logs, timestamps, Hash sums
- Postmortems: blameless, with concrete fixes

SECURITY FOR SALES: PROOF & ASSURANCE

Prospects will ask for proof. Maintain a lightweight security packet: policies, architecture diagrams, control summaries, and third-party attestations where possible. This shortens security questionnaires and accelerates deals.

- Packet: security overview, subprocessor list, controls map
- Evidence: pen tests, vulnerability scans, training logs
- FAQ: breach history, backup/restore RTO/RPO
- Outcome: fewer blockers, faster procurement

ETHICAL DATA USE

ETHICS: BEYOND COMPLIANCE

Compliance sets the floor; ethics sets the bar. Ethical data use means respecting users' expectations, avoiding manipulation, and designing for fairness. It is a strategic choice that differentiates your brand in crowded markets.

- Principles: respect, fairness, transparency, accountability
- Practice: explain choices; avoid dark patterns
- Benefit: loyalty and positive word of mouth
- Risk: short-term gains vs. long-term trust

FAIRNESS & BIAS IN DATA AND AI

Datasets encode history's biases. When models inherit them, outcomes can be unfair. Address this proactively by curating data, auditing models, and providing recourse.

- Actions: representative samples, bias testing, monitoring drift
- Safeguards: human review for high-stakes decisions
- Documentation: model cards, data sheets
- User recourse: appeals and explanations

TRANSPARENCY & CONSENT UX

Users deserve clarity about what data you collect and why. Write privacy notices in plain language, offer meaningful choices, and let users revisit settings easily. Good consent flows increase trust and reduce support burdens.

- Design: layered notices, just-in-time prompts
- Choices: opt-in for non-essential processing
- Controls: dashboards for preferences & deletions
- Test: comprehension with real users

DATA SHARING & PARTNERSHIPS

Sharing data with partners can create value, but it must be justified, minimized, and controlled. Use contracts, technical safeguards, and periodic reviews to ensure shared data serves users' interests.

- Limit: purpose-bound, minimal fields, retention caps
- Secure: encryption, access logs, segregation
- Review: audits and termination clauses
- Inform: clear disclosures to users

ETHICS IN GROWTH & MARKETING

Growth can be ethical: target relevance over intrusion, frequency caps over fatigue, and clear opt-outs. Respect do-not-track signals and avoid manipulative countdowns or hidden fees.

- Guardrails: frequency limits, sane defaults
- Honesty: total price upfront, no bait-and-switch
- Respect: easy unsubscribe, no forced consent
- Measure: satisfaction and trust—not only clicks

KEY TAKEAWAYS

Security, privacy, and ethics are accelerators, not brakes. A small set of smart controls, clear legal grounding, and humane data practices build durable trust. Start lean, document decisions, automate what you can, and iterate as you grow.

- Trio: lawful processing, strong controls, ethical design
- Start small: top 10 controls + RoPA + DPIA where needed
- Prove it: logs, audits, artifacts
- Culture: everyone owns security & privacy

Become Busy Xelerator

THANK YOU

Project number: 2023-1-EL02-KA220-YOU-000160907

www.becomebusy.eu www.fifty-fifty.gr

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the Youth and Lifelong Learning Foundation (INEDIVIM). Neither the European Union nor the granting authority can be held responsible for them.