DEFENDERS

Defending VET Students within Cybersecurity Innovation

MODULE 6: CYBERSECURITY COMPLIANCE AND LEGAL ASPECTS

Project No: 2025-1-PL01-KA210-VET-000363642

www.defenders-project.eu

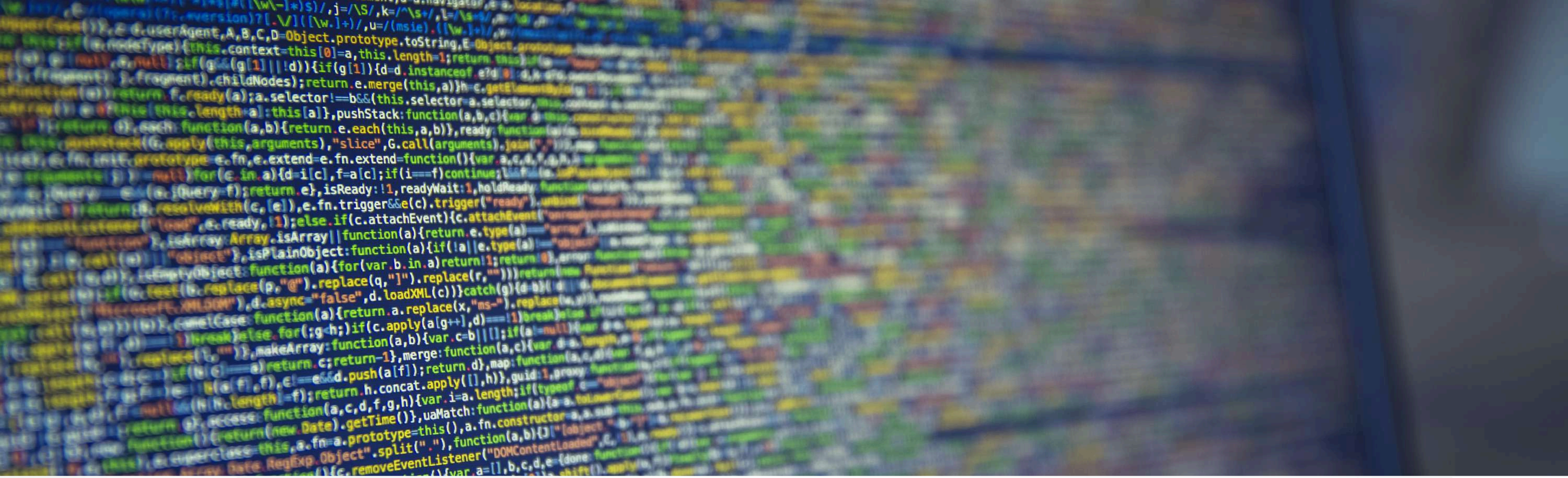
FUNDACJA ROZWOJU SPOŁECZNEGO CIVITAS

M.S.A. ΚΕΝΤΡΟ ΔΙΑ ΒΙΟΥ ΜΑΘΗΣΗΣ

NIKOLA KAREV State High School & VET Centre Strumica

Co-funded by the European Union

Funded by the EU. The views and opinions expressed are solely those of the author(s) and do not necessarily reflect the views and opinions of the European Union or the Foundation for the Development of the Education System. Neither the European Union nor the Foundation for the Development of the Education System are responsible.

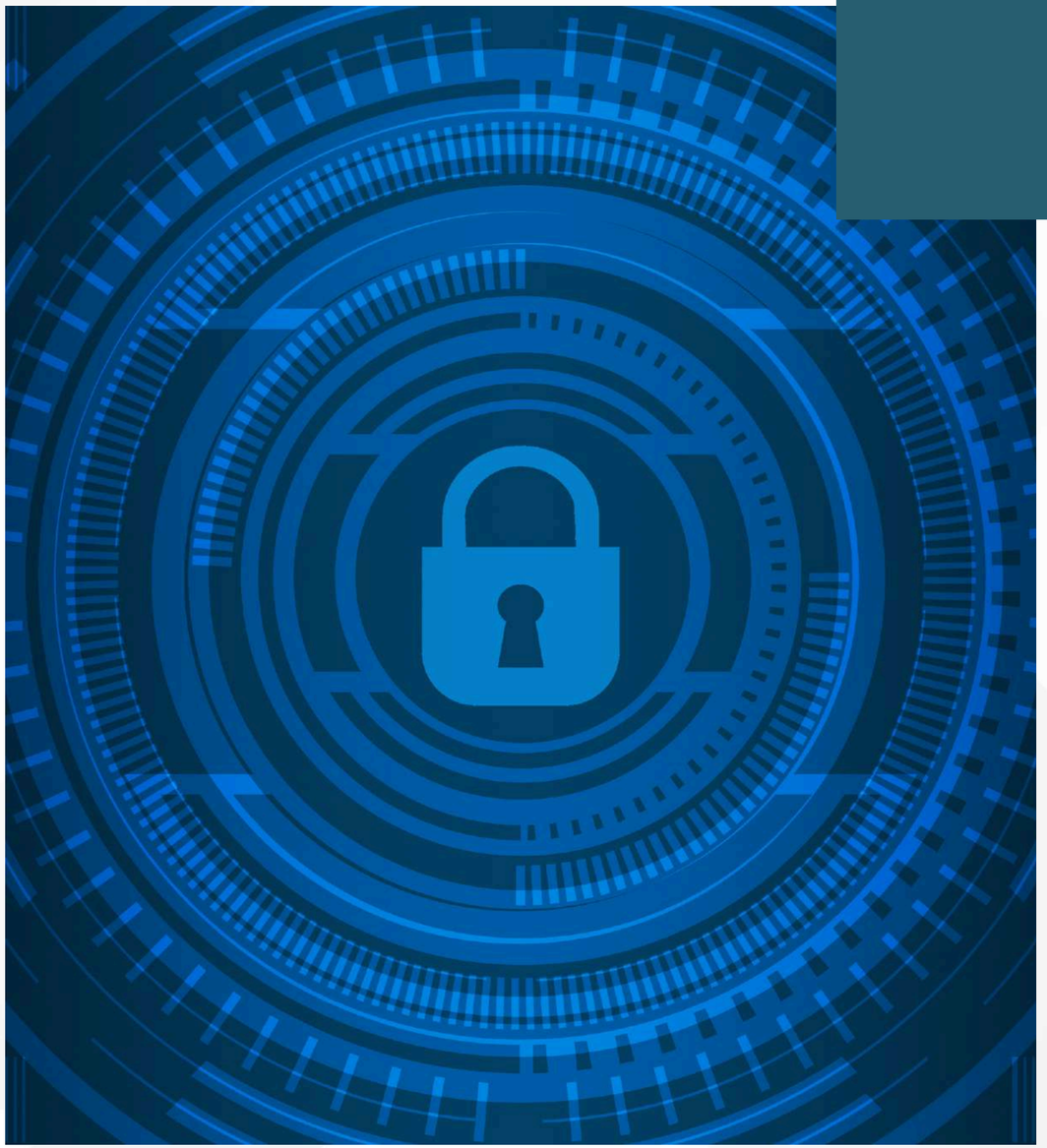


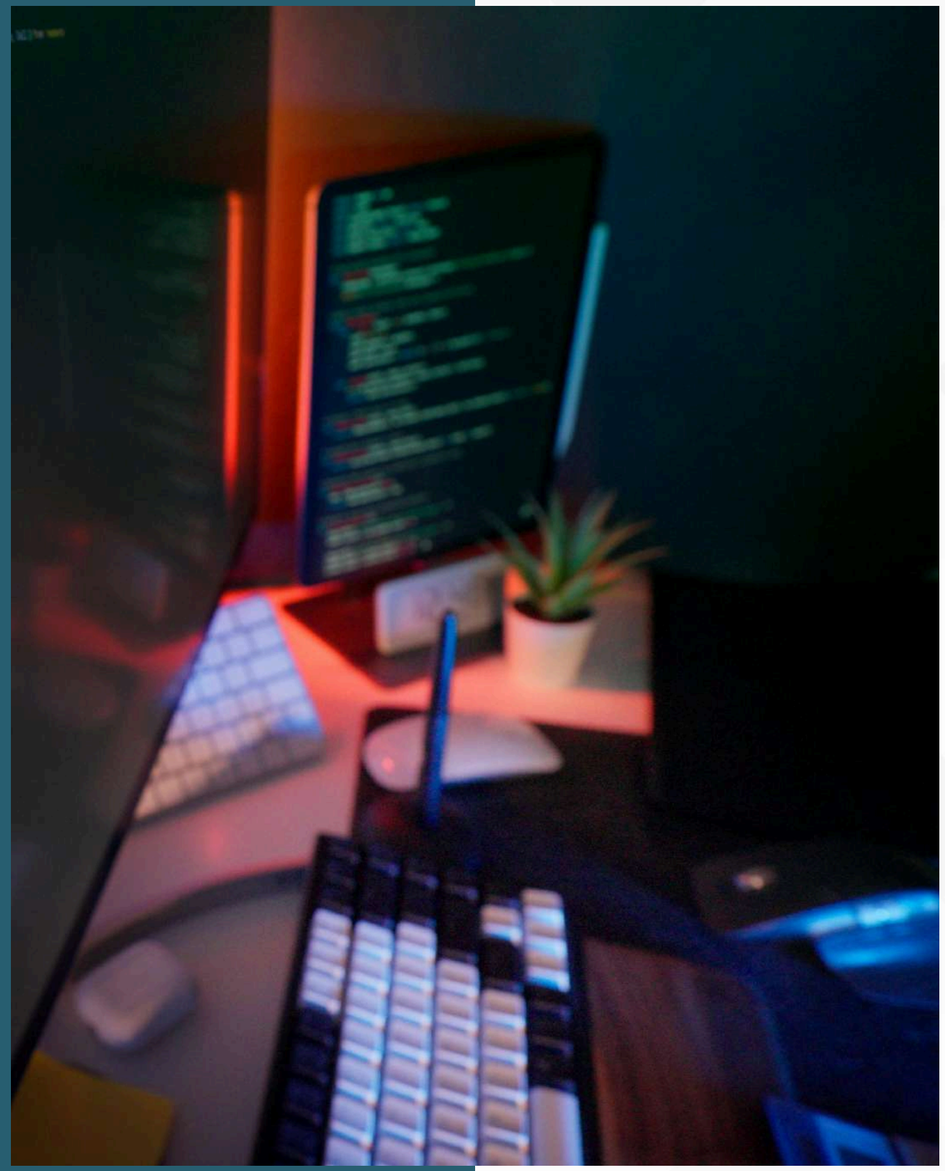
LEARNING PATH

From legal vocabulary to real organisational decisions.

EXECUTIVE SUMMARY

- Cybersecurity compliance is no longer an IT appendix; it is a core institutional duty.
- Module 6 connects GDPR, NIS2/KSC, incident reporting, evidence preservation and governance.
- The VET setting is treated as a real operational environment: LMS, e-registers, internships, cloud tools, partner data.
- The result: participants know who acts, when, how, and why.





INTRODUCTION

- Compliance is the capacity to make correct decisions under pressure, not a shelf of policies.
- VET institutions process personal, educational, employment and sometimes health-related data.
- Digital continuity matters: a compromised LMS or gradebook is not an inconvenience — it is institutional disruption.
- The module translates law into operational practice.

OVERVIEW

- Regulatory harmonisation: GDPR + NIS2 + Polish KSC logic.
- Role clarity: controller, processor, DPO, management, IT, teacher, student.
- Incident qualification: security event, personal data breach, serious/significant incident.
- Practical readiness: reporting clocks, records, evidence, tabletop exercises.

1
Legal roles

2
Risks & assets

3
Data breaches

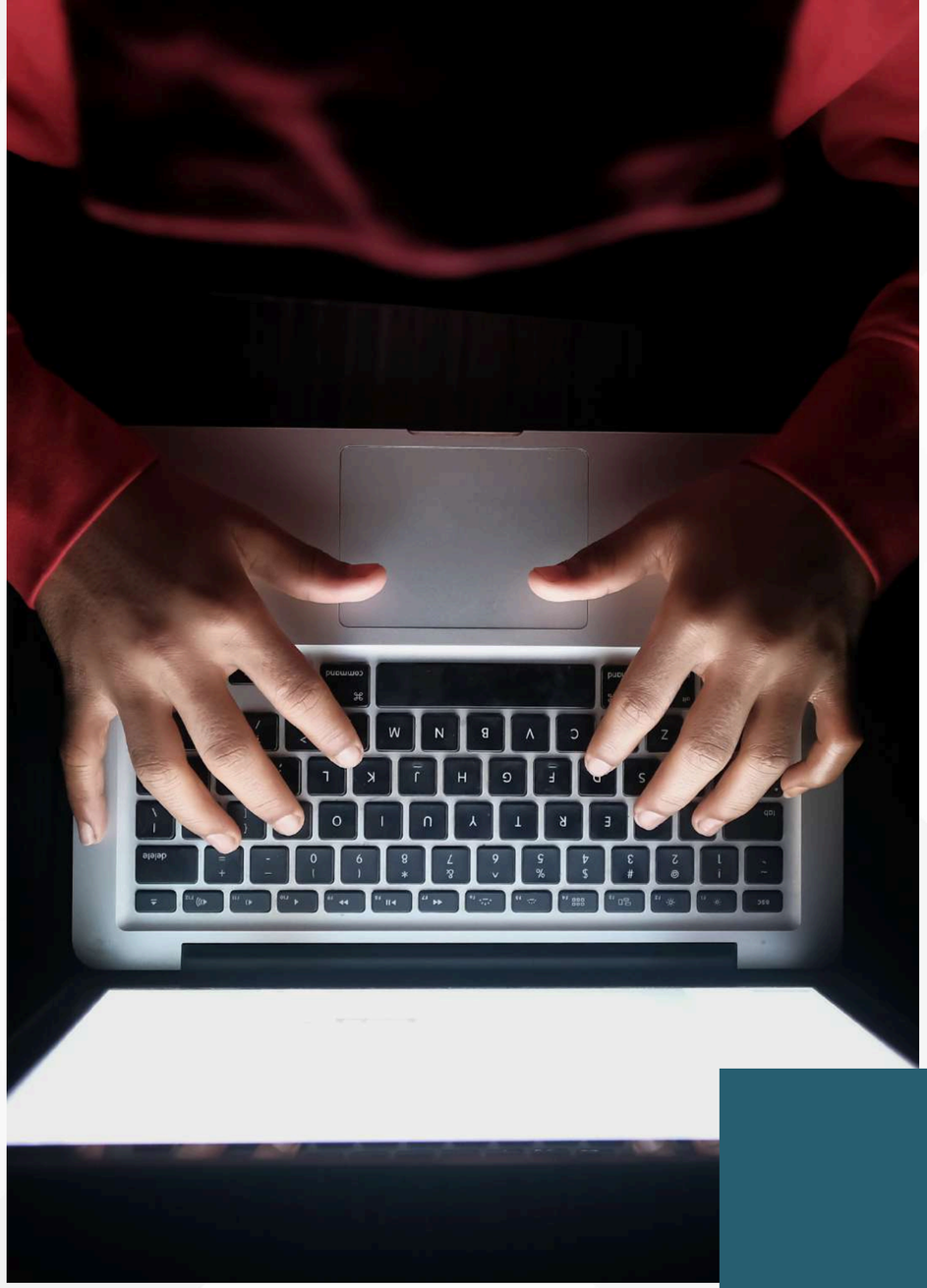
4
NIS2/KSC

5
Evidence

6
Governance

WHY THIS TOPIC MATTERS

- **Legal exposure:** GDPR breach notification and documentation duties.
- **Operational exposure:** ransomware, account takeover, LMS downtime.
- **Reputational exposure:** trust of students, parents, staff and employers.
- **Governance exposure:** management accountability and procurement duties.
- **Evidence exposure:** poor logs can make investigation legally and technically weak.
- **Pedagogical exposure:** students learn security culture from institutional practice.

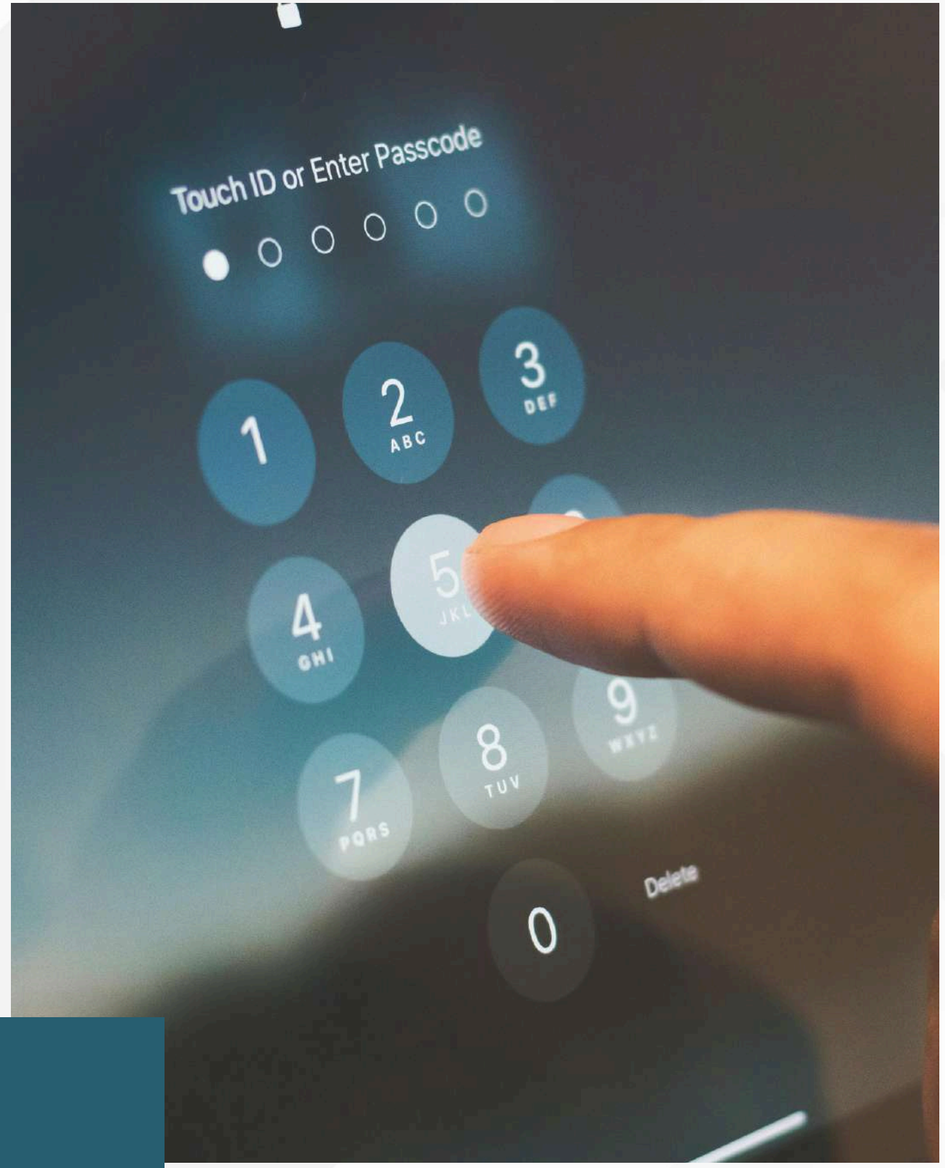


LEARNING OBJECTIVES

LO1	Differentiate controller, processor, joint controllers and Data Protection Officer responsibilities.
LO2	Classify events as security incidents, personal data breaches, or serious/significant incidents.
LO3	Apply GDPR and NIS2/KSC notification logic, including 72h and staged reporting clocks.
LO4	Prioritise VET assets and choose proportionate controls: access, backups, encryption, logging and vendor clauses.
LO5	Preserve forensic evidence and communicate professionally during and after an incident.

KEY CONCEPTS AND DEFINITIONS

- **GDPR / RODO** — EU legal framework for personal data protection, security of processing and breach notification.
- **NIS2** — EU framework for cyber resilience of essential and important entities, including governance and reporting duties.
- **KSC** — Polish national cybersecurity system; project materials include the S46 reporting path.
- **CIA triad** — confidentiality, integrity and availability; a practical language for breach qualification.
- **ISMS / SZBI** — structured information security management system based on risk and accountability.

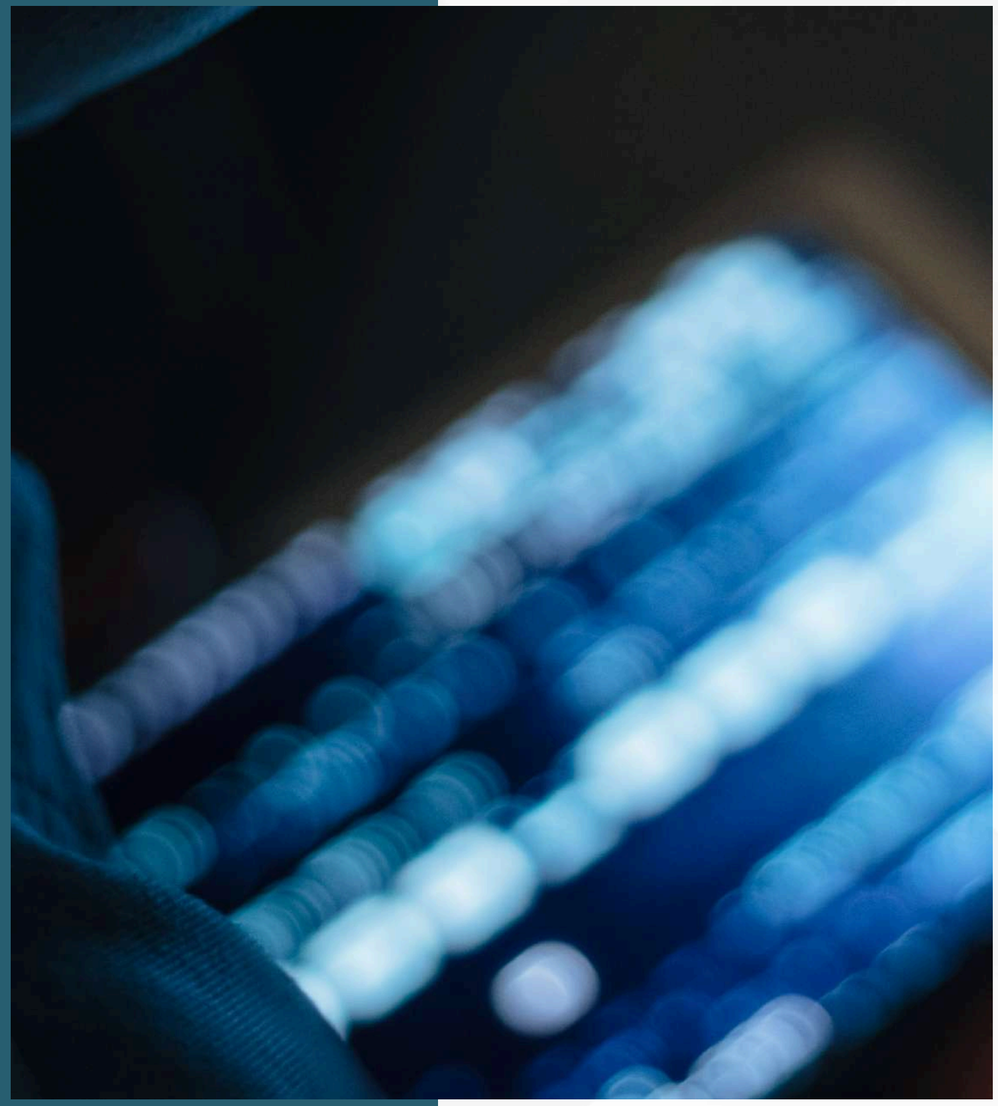


CONTEXT: VET AS A DATA-RICH ENVIRONMENT

- VET institutions combine education, administration, internships, laboratories and employer cooperation.
- Typical assets: LMS, e-registers, gradebooks, attendance systems, internship documentation, cloud drives, identity systems, backups.
- The practical problem: fast informal reporting may help reaction but weakens documentation and lessons learned.
- The module therefore builds role-based habits: report early, document clearly, preserve evidence.

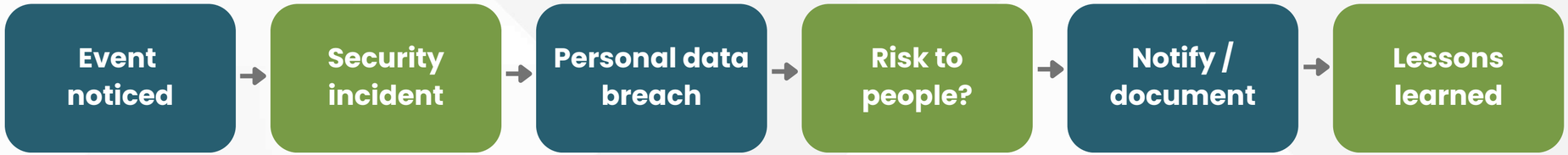
MAIN THEME 1: LEGAL ROLES

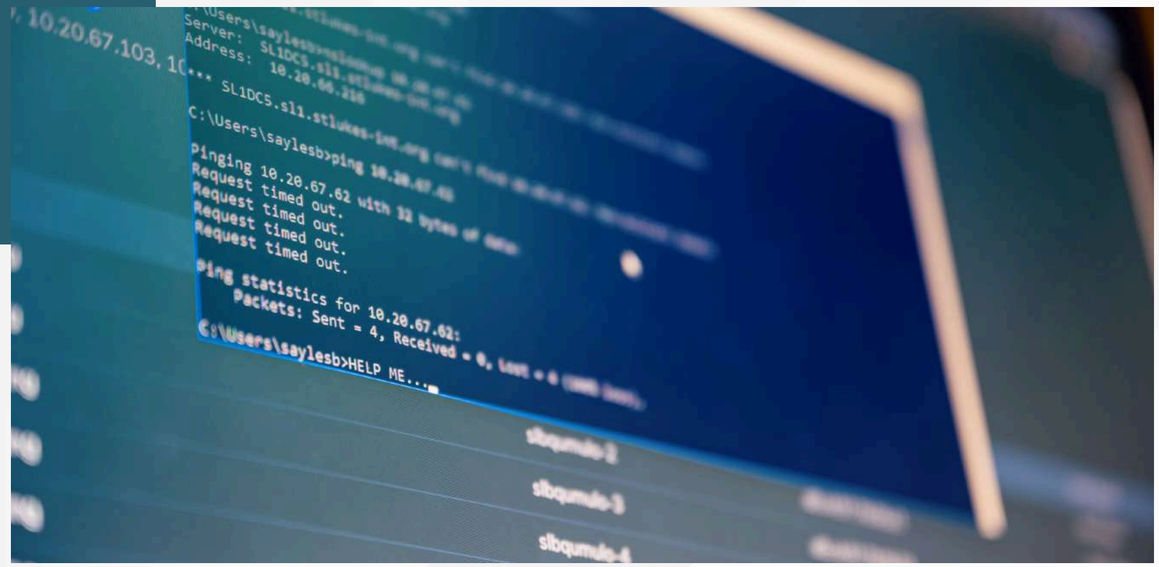
Controller	Determines purposes and means of processing; owns breach assessment and accountability.
Processor	Processes on documented instructions; must support security and incident response.
DPO	Advises, monitors, raises risks; does not replace management responsibility.
Management	Approves resources, accepts risk, ensures governance and compliance culture.
Users	Report anomalies, follow procedures, protect credentials and devices.



MAIN THEME 2: BREACH QUALIFICATION

- Not every security event is a personal data breach; every personal data breach must be documented.
- Confidentiality breach: unauthorised access or disclosure.
- Integrity breach: unauthorised alteration of data.
- Availability breach: loss of access or destruction of data.





MAIN THEME 3: REPORTING CLOCKS

- Do not wait for perfect certainty; start an evidence trail and involve the responsible roles.
- GDPR notification depends on risk to rights and freedoms of people.
- NIS2/KSC reporting depends on entity status and incident significance.
- Internal recordkeeping is mandatory even when external notification is not required.

0–15 min
Detect & escalate

→

24h
Early warning*

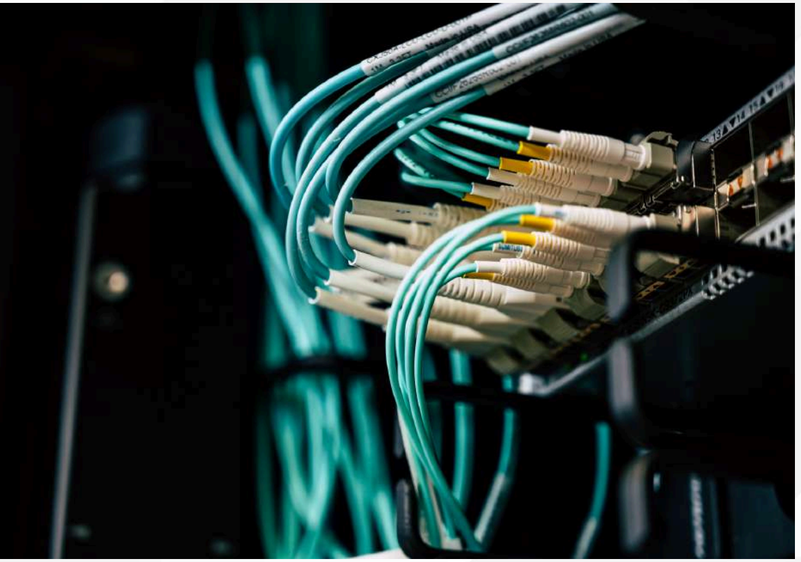
→

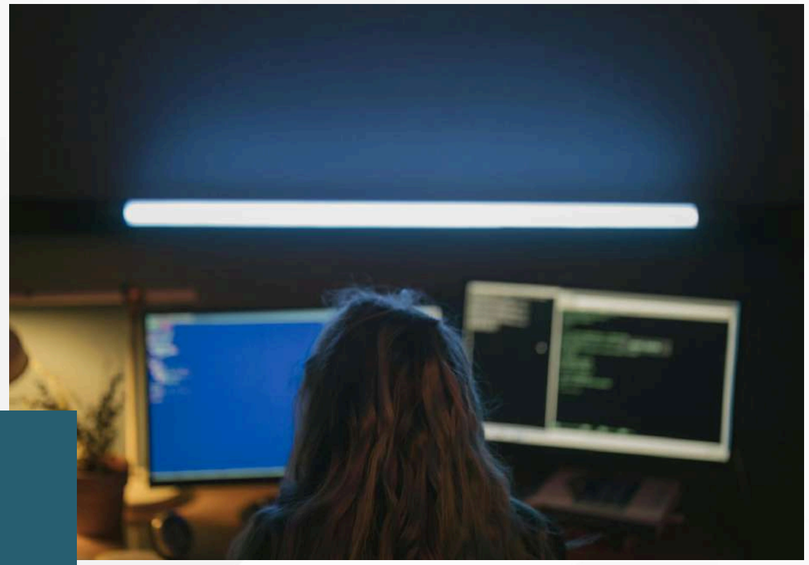
72h
GDPR / incident notice

→

1 month
Final report*

*For NIS2/KSC-style staged reporting where applicable in the institutional context.



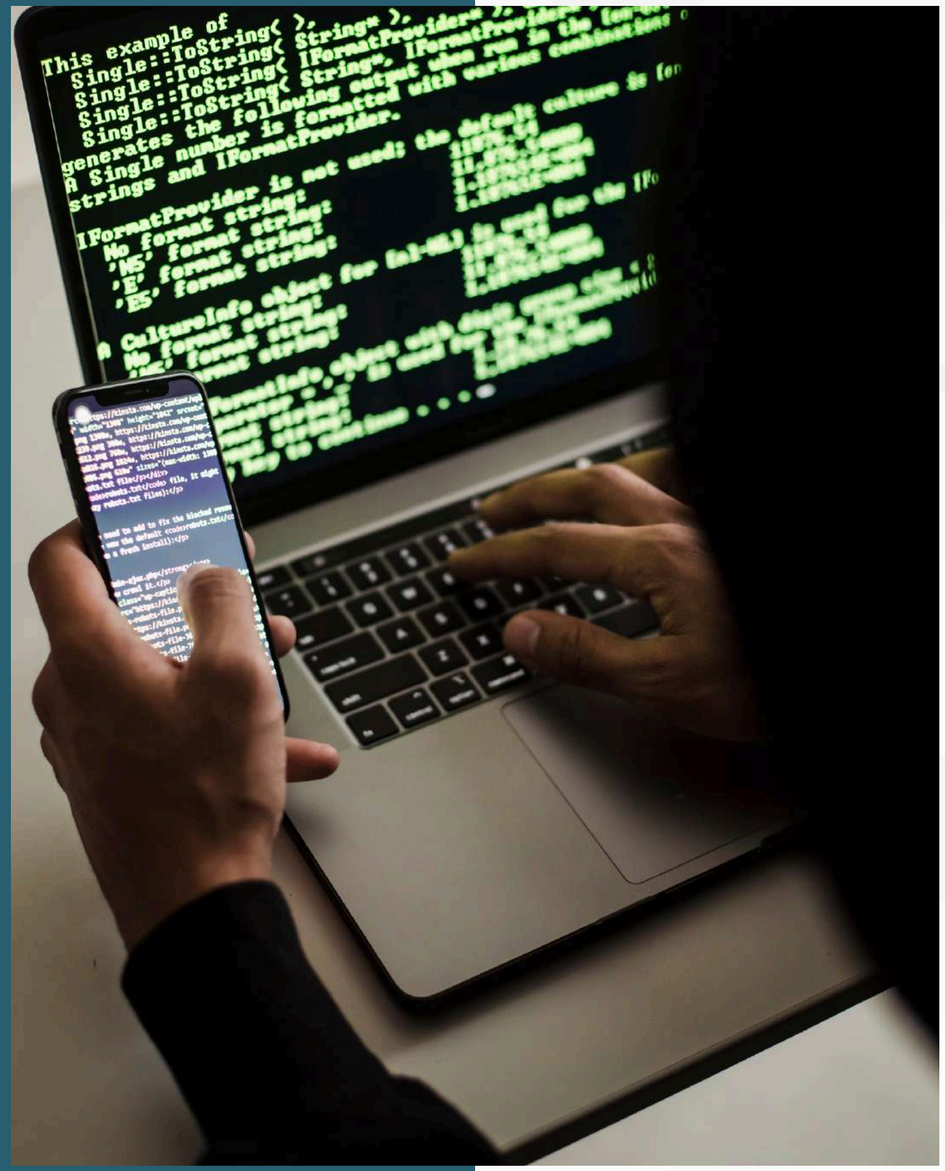


CORE PRINCIPLES

- **Risk-based proportionality:** strongest controls for highest-risk data.
- **Accountability:** decisions must be documented and defensible.
- **Data minimisation:** collect and share only what is needed.
- **Need-to-know access:** role-based permissions and MFA.
- **Evidence integrity:** logs, timestamps, hash manifests and chain of custody.
- **No-blame reporting:** fast escalation beats elegant silence.
- **Vendor discipline:** contracts must include security and breach cooperation.
- **Continuous improvement:** every incident becomes a lesson.

CHALLENGES AND RISKS

- **Role confusion:** “IT will handle it” is not a compliance model.
- **Informal reporting:** quick, but often invisible and legally weak.
- **Weak logging:** no logs, no timeline; no timeline, no reliable investigation.
- **Cloud and SaaS sprawl:** free tools may create uncontrolled processing.
- **Supply chain dependency:** processors must be ready to support breach assessment.
- **Human pressure:** fear of blame delays reporting, and delays multiply damage.



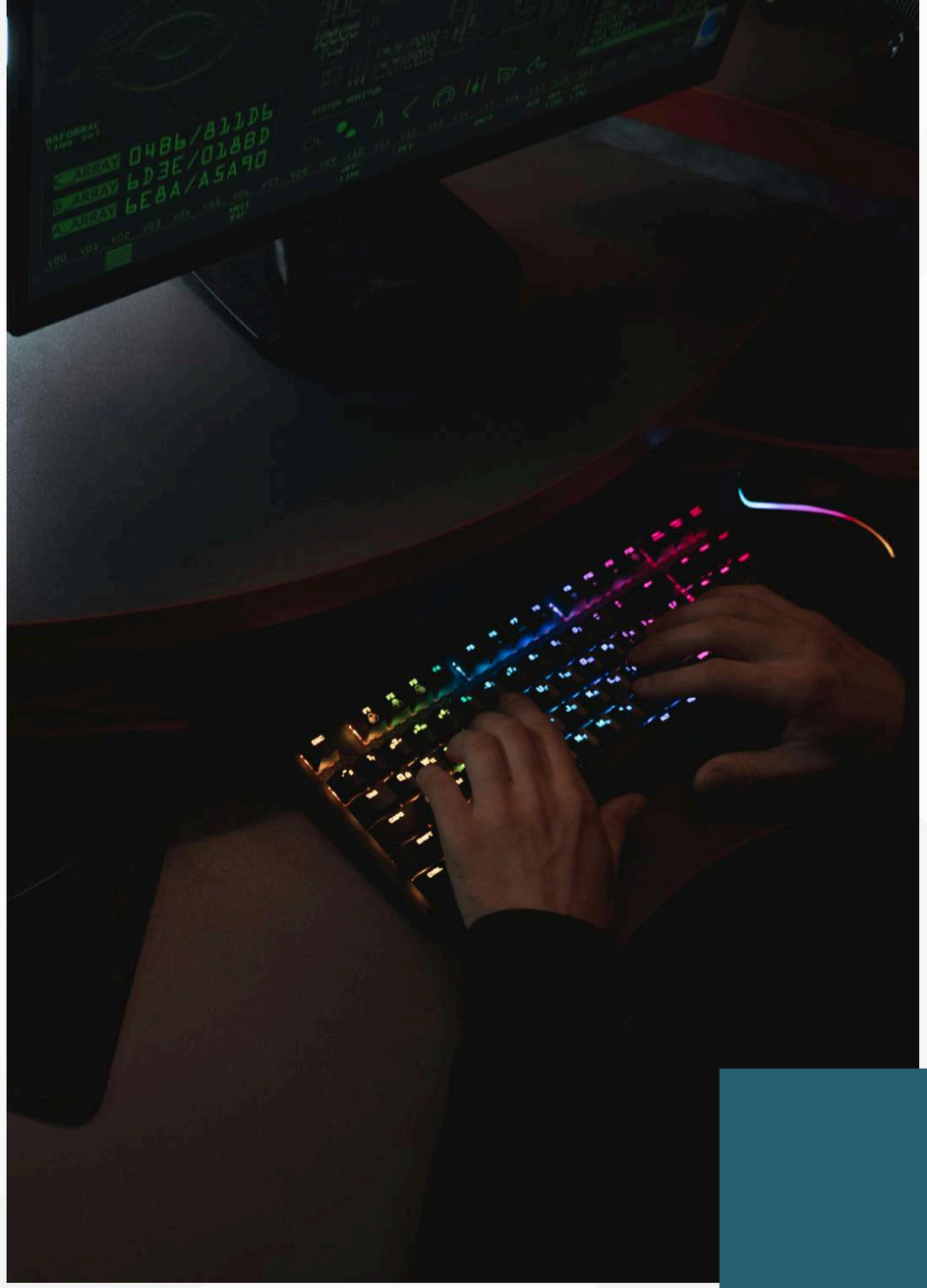
OPPORTUNITIES AND BENEFITS

- **Compliance as resilience:** fewer surprises, faster decisions, better continuity.
- **Better employer trust:** secure VET partners are easier to invite into real projects.
- **Better learning culture:** students experience professional security practice, not slogans.
- **Better procurement:** contracts become instruments of risk control.
- **Better management:** board-level awareness turns cybersecurity into a normal governance topic.

PRACTICAL APPLICATION: ASSET CLASSIFICATION

P1 Public	Website content, cafeteria menu, public course catalogue.
P2 Internal	Staff procedures, internal schedules, non-sensitive operational notes.
P3 Restricted	Grades, attendance, internship evaluations, staff HR data.
P4 Critical	Health/psychological support data, admin credentials, identity records, incident evidence.

Decision rule: the higher the risk to people and institutional continuity, the stronger the control package: MFA, encryption, backup, audit logs, restricted sharing.



TOOLS AND METHODS

- Incident register and breach assessment form.
- RACI matrix for controller, DPO, IT, management and communications.
- Data-processing agreement checklist for processors.
- Asset register and classification labels.
- SIEM / log management for correlation and audit trails.
- EDR/MDR for endpoint detection and response.
- MITRE ATT&CK mapping for attacker behaviour.
- P-DEFSOP-style evidence workflow: collect, preserve, analyse, report.

FORENSIC READINESS: BEFORE THE INCIDENT

- Forensic readiness means being able to collect, preserve and use digital evidence efficiently.
- SMEs and VET-like organisations often lose evidence because logs are absent, overwritten or undocumented.
- Practical minimum: log sources, retention rules, access control, export procedure, chain-of-custody record.

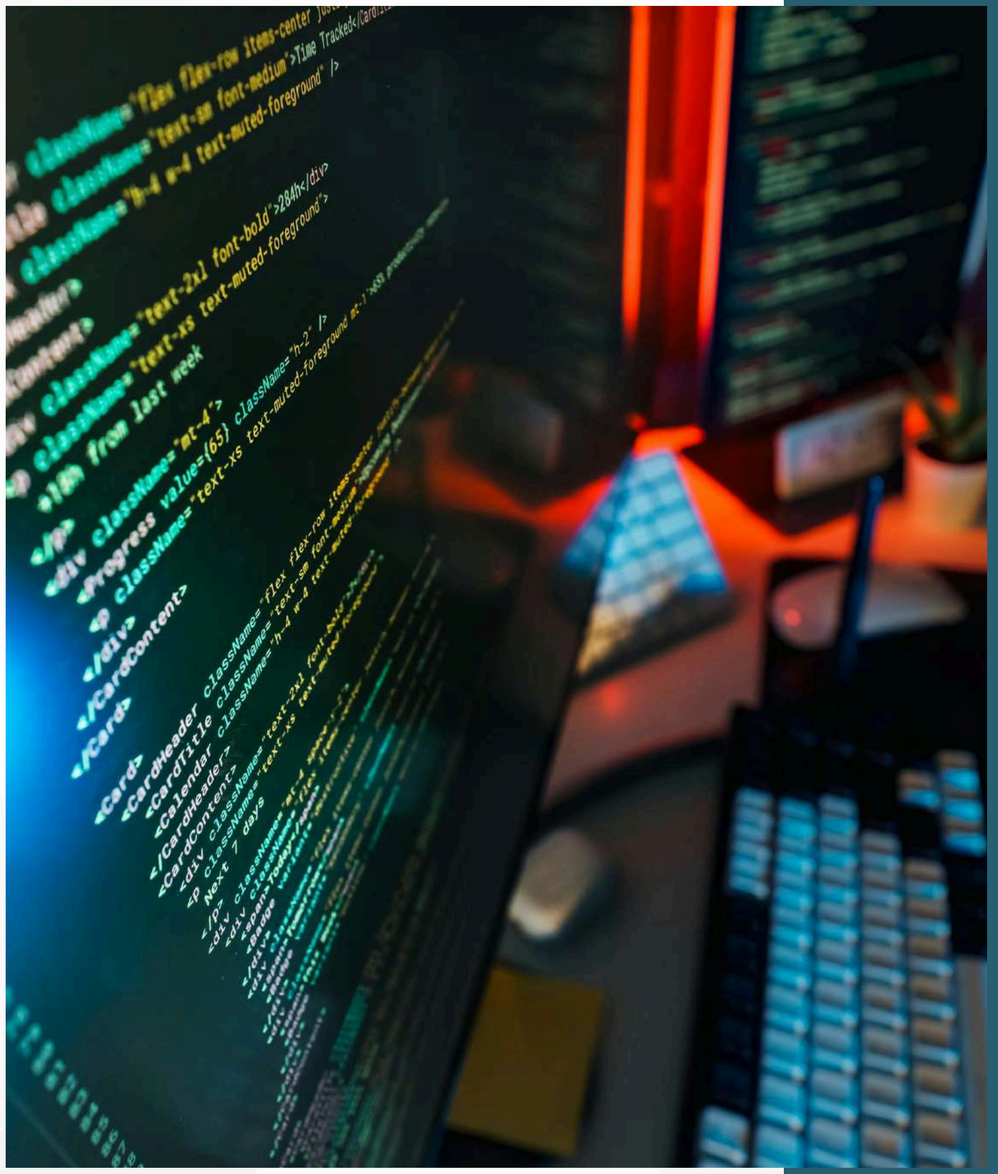
PROACTIVE DIGITAL FORENSICS: P-DEFSOP LOGIC

Reactive	Starts after the incident; evidence may already be incomplete.
DEFSOP	Provides structured digital evidence procedure and documentation.
P-DEFSOP	Pre-positions collectors, maps rules to ATT&CK, secures custody and measures coverage.
ISO alignment	Supports incident management and legal admissibility of evidence.

The practical lesson for VET: incident response starts long before the incident. Otherwise the first evidence is panic, and panic is a poor forensic tool.

DETECTION: SIEM, EDR AND GRAPH THINKING

- SIEM centralises security-relevant events for correlation, alerting, investigation and reporting.
- EDR records host-level behaviour: process launches, network connections, file changes, registry activity and command lines.
- Graph-based detection uses relationships between files, processes, domains and infrastructure to identify suspicious “unknown knowns”.
- This supports compliance because detection, investigation and reporting become evidence-based.



CASE SCENARIO: RANSOMWARE IN A VET SCHOOL

- Monday, 10:00 — a teacher reports that the LMS is unavailable and a shared drive shows encrypted filenames.
- 10:15 — IT confirms suspicious login from an external IP and possible access to student internship evaluations.
- 10:30 — management, DPO and communications lead open an incident log.
- Key question: Is this only service disruption, a personal data breach, a serious cyber incident, or all of them?

SCENARIO DECISION MAP

Contain accounts → **Preserve logs** → **Assess data** → **Notify roles** → **Decide reporting** → **Recover & learn**

- Immediate containment must not destroy evidence: avoid “cleaning” before exporting critical logs.
- DPO supports breach risk analysis: type of data, number of persons, sensitivity, likely consequences.
- Management decides and documents notifications, resources and external communication.
- Post-incident: update controls, contracts, training and backup procedures.

INTERACTIVE ACTIVITY 1: 24-HOUR CLOCK CHALLENGE

- Teams receive a short incident log and a role card: management, DPO, IT, teacher, communications.
- Task: prepare an early warning / first internal briefing in 20 minutes.
- Must include: what happened, affected systems, possible personal data, immediate measures, missing information, next deadline.
- Debrief: what was certain, what was uncertain, what evidence was needed?

INTERACTIVE ACTIVITY 2: DATA CLASSIFICATION ESCAPE ROOM

- Participants classify five VET data items: public course catalogue, staff schedule, student grades, internship evaluations, psychological support notes.
- For each item, they choose storage location, access level, sharing rule and breach response priority.
- Success condition: at least four correct classifications and one justified control per item.
- Debrief: which data looked harmless but carried risk?

REFLECTION POINTS

- Would I report an accidental data exposure immediately, or would I first try to hide the embarrassment?
- Do our everyday communication channels leave an evidence trail?
- Do we know where student data is stored when we use a free tool?
- Could we explain our first 72 hours of action to students, parents, employers and regulators?
- Which fear in our institution slows down honest reporting?

KEY TAKEAWAYS

- Compliance is dynamic: it is a cycle of risk, control, detection, reporting and improvement.
- Roles matter: DPO advises, management decides, IT supports, users report.
- • Reporting clocks are unforgiving; evidence must start immediately.
- Risk-based logic wins: protect sensitive and critical assets first.
- People are not the weakest link by nature; badly designed systems make them look that way.

SUMMARY

- Module 6 turns legal obligations into operational competence for VET institutions.
- Participants learn to identify roles, classify data, assess breaches, preserve evidence, and choose the right notification path.
- The central competence is practical judgement under time pressure.
- The desired institutional culture is not fear of mistakes, but disciplined responsibility.

ASSESSMENT / REVIEW

- **Formative quiz:** roles, CIA triad, breach thresholds, reporting deadlines.
- **Practical task:** complete an incident register entry and justify notification decision.
- **Tabletop assessment:** produce a short final incident report and communication note.
- **Pass criteria:** correct role mapping, reasonable risk analysis, 72h pathway, and at least three preventive measures.

CONCLUSION

- A VET institution is cyber-resilient when its people know what to do before the lawyers arrive.
- The first 15 minutes, the first 24 hours and the first 72 hours must be designed, trained and documented.
- Compliance is not bureaucracy for its own sake; it is organised trust.
- The module should be delivered as a workshop: short input, role exercise, case analysis, tabletop, review.

DEFENDERS

Defending VET Students within Cybersecurity Innovation

MODULE 6: CYBERSECURITY COMPLIANCE AND LEGAL ASPECTS

Project No: 2025-1-PL01-KA210-VET-000363642

www.defenders-project.eu

FUNDACJA ROZWOJU SPOŁECZNEGO CIVITAS

M.S.A. ΚΕΝΤΡΟ ΔΙΑ ΒΙΟΥ ΜΑΘΗΣΗΣ

NIKOLA KAREV State High School & VET Centre Strumica

Co-funded by the European Union

Funded by the EU. The views and opinions expressed are solely those of the author(s) and do not necessarily reflect the views and opinions of the European Union or the Foundation for the Development of the Education System. Neither the European Union nor the Foundation for the Development of the Education System are responsible.