

EU Artificial Intelligence, Data & Digital Governance Certification Handbook



ECVC | European Centre for
Vocational Certification

www.ecvc.eu

2026

This handbook provides candidates with comprehensive information about the ECVC EU Artificial Intelligence, Data & Digital Governance Certification Programme. It is designed to help candidates understand the available certifications and select the certification that best corresponds to their knowledge, professional experience, and development objectives in EU artificial intelligence, data protection, privacy, and digital governance.

For each certification, the handbook presents its purpose and scope, key benefits, learning objectives, target audience, study materials, exam format and difficulty level, exam outline, and prerequisites. It also explains how the certifications address different areas of professional competence, from applying EU data protection requirements and ethical AI principles to advanced AI governance, regulatory compliance, and privacy management in AI systems.

Candidates are strongly encouraged to read this handbook in full before registering for a Certification Exam.

For all technical-related inquiries, please contact support@ecvc.eu.

Table of Contents

A.	About ECVC	2
B.	Overview of the EU Artificial Intelligence, Data & Digital Governance Certification Programme.....	3
C.	Overview of Certified EU Data Protection and Privacy Officer (EUDP ² O)	4
	C.1. Key Benefits	5
	C.2. Learning Objectives	6
	C.3. Target Audience.....	7
	C.4. Study Material	8
	C.5. Exam Format & Difficulty Level	8
	C.6. Exam Outline	9
	C.7. Prerequisites	9
D.	Overview of the Certified EU AI Governance & Compliance Specialist (EUAIGO).....	10
	D.1. Key Benefits.....	11
	D.2. Learning Objectives	12
	D.3. Target Audience	13
	D.4. Study Material	14
	D.5. Exam Format & Difficulty Level	14
	D.6. Exam Outline.....	15
	D.7. Prerequisites	16
E.	Overview of the Certified EU Ethical AI Practitioner (ETHAI).....	16
	E.1. Key Benefits	17
	E.2. Learning Objectives	18
	E.3. Target Audience	19

E.4. Study Material	19
E.5. Exam Format & Difficulty Level	20
E.6. Exam Outline	20
E.7. Prerequisites	21
F. Overview of the Certified EU AI Data Protection & Privacy Professional (AIDData)	22
F.1. Key Benefits	22
F.2. Learning Objectives	24
F.3. Target Audience	26
F.4. Study Material	27
F.5. Exam Format & Difficulty Level	28
F.6. Exam Outline	28
F.7. Prerequisites	29

A. About ECVC

The European Centre for Vocational Certification (ECVC) is a leading authority in providing globally recognized certifications across a wide range of high-demand fields. Our mission is to empower individuals and organizations through cutting-edge, industry-relevant qualifications that reflect excellence and support professional success in today's competitive environment.

Rooted in European Union legislation, policies, and official publications, ECVC certifications not only meet global standards but are also closely aligned with the regulatory frameworks and policy guidelines that shape professional practices within the EU.

ECVC is more than just a certification provider, we are a dedicated partner in your professional journey. With a strong commitment to quality and innovation, we strive to make your certification experience both meaningful and transformative. Our programs are designed to strengthen your knowledge, enhance your skills, and support your career advancement.

B. Overview of the EU Artificial Intelligence, Data & Digital Governance Certification Programme

ECVC offers a comprehensive EU Artificial Intelligence, Data & Digital Governance Certification Programme covering different levels of professional knowledge, competence, and experience, with certifications corresponding to relevant European Qualifications Framework (EQF) levels. These certifications are developed and delivered in line with high quality standards, with all certification-related activities managed through the ECVC exam platform.

The certifications assess candidates' understanding of European Union legislation, regulatory requirements, and governance frameworks relating to artificial intelligence, data protection, privacy, and responsible digital technologies. The examinations focus on interpreting and applying the EU AI Act, General Data Protection Regulation (GDPR), and related EU legislation, policies, and official guidance. Key areas of assessment include ethical and trustworthy AI, data protection principles, AI risk management, regulatory compliance, transparency, accountability, human oversight, and organisational governance. Candidates are expected to demonstrate an appropriate level of knowledge and applied competence in addressing legal, ethical, and operational requirements within their professional environments.

Together, these certifications support the development of specialised knowledge and practical capability across EU artificial intelligence, data protection, and digital governance. They provide opportunities for professionals to strengthen their understanding of EU regulatory frameworks, apply responsible AI and privacy principles, and develop advanced competence in governance and compliance. The programme covers different areas of specialisation and competence levels, supporting professional development from practical implementation to advanced regulatory oversight and organisational governance. It also helps organisations strengthen internal

expertise, manage regulatory risks, and promote responsible, transparent, and accountable use of AI and data-driven technologies.

C. Overview of Certified EU Data Protection and Privacy Officer (EUDP²O)

The Certified EU Data Protection and Privacy Officer (EUDP²O) is an ECVC credential that validates the ability to interpret and apply EU privacy law, with a primary focus on the GDPR and related EU instruments. The exam confirms competency in reading law and guidance, designing and monitoring controls, advising on lawful bases and rights, conducting DPIAs, and coordinating incident and breach response. The scope covers authoritative EU legislation, policies, and supervisory guidance, translated into practical day to day operations. Candidates gain learning outcomes that include risk based decision making and accountability by design. Successful candidates earn a title that signals professional credibility and impact across the EU. The certification corresponds to EQF Level 5[1.1], reflecting specialised practical competence in applying EU data protection and privacy requirements in day-to-day operations.

It also supports organisations in strengthening privacy governance and building reliable processes for compliance with EU data protection obligations. It helps translate GDPR requirements into consistent operational practice, including data flow mapping, privacy by design, records of processing, data retention, lawful basis assessment, vendor oversight, DPIAs, and breach response. It also supports stronger accountability, better audit readiness, and more effective engagement with supervisory authorities, while helping organisations align privacy and security controls across business functions.

For individuals, this certification demonstrates recognised competence in EU data protection and privacy practice and supports the ability to turn legal and

regulatory requirements into clear procedures and practical advice. It is particularly relevant for those working in data protection, privacy, compliance, legal, risk, security, and governance roles, as well as for professionals preparing for DPO or privacy leadership responsibilities. It also strengthens professional credibility and supports more effective collaboration with legal, security, and technical teams.

C.1. Key Benefits

For Organisations

EUDP²O helps organisations turn EU privacy obligations into reliable operations that withstand audits and regulatory scrutiny. Certified practitioners can interpret GDPR requirements, map data flows, embed privacy by design, and maintain evidence for accountability. They help select lawful bases, manage vendor risk, and operationalise DPIAs and breach response. This reduces incident likelihood, shortens investigation timelines, and supports consistent decision making across business units and countries. Certified staff improve the quality of privacy notices, records of processing, and retention rules. They align security and privacy controls, improving resilience and trust with customers and partners. The certification also supports board level assurance by linking policies to measurable controls and by preparing teams for supervisory authority engagement.

For Individuals

The certification signals verified competence in EU data protection and privacy practice. Candidates demonstrate the ability to read law and guidance, translate obligations into procedures, and advise stakeholders with confidence. The certification strengthens career mobility across the EU by providing a recognised benchmark of skills. It helps professionals step into DPO roles or privacy leadership by proving capability in DPIAs, incident handling, vendor oversight, and records management. Holders gain a common vocabulary for working with legal, security, and engineering teams, which

increases influence and effectiveness. The program supports continuous learning, keeping skills aligned to evolving guidance and case law. Certified professionals gain credibility with clients, regulators, and internal decision makers.

C.2. Learning Objectives

By completing this certification, candidates will be able to:

- Interpret GDPR provisions using articles, recitals, EDPB guidance, and relevant case law.
- Translate legal requirements into practical policies, procedures, and controls.
- Map processing activities and maintain records of processing and data inventories.
- Select and document lawful bases, including legitimate interests with an Legitimate Interests Assessment.
- Embed privacy by design and by default across projects and product lifecycles.
- Conduct and document DPIAs and choose proportionate risk mitigations.
- Operationalise data subject rights with clear intake, verification, and response workflows.
- Manage vendors through DPAs, due diligence, and continuous monitoring.
- Assess and govern international data transfers and safeguards.
- Coordinate incident response and breach notification with security teams.
- Measure, report, and improve privacy performance and accountability.
- Train staff and stakeholders and build a privacy culture.

- Advise leadership and collaborate effectively with DPOs and supervisory authorities.
- Maintain auditable evidence that demonstrates sustained compliance.

C.3. Target Audience

This certification is ideal for:

- Current or aspiring Data Protection Officers and deputies.
- Privacy managers, analysts, and compliance officers in EU based or EU facing organisations.
- In house legal counsel and contract managers who draft or review DPAs and privacy terms.
- Information security, risk, and GRC professionals who align controls with GDPR requirements.
- Product and engineering leads who implement privacy by design and default.
- IT service owners and data architects responsible for data inventories and retention.
- Marketing, CRM, and analytics teams that rely on consent and legitimate interests.
- HR and People Operations handling employee data across multiple jurisdictions.
- Procurement and vendor management teams overseeing processors and sub processors.
- Auditors and consultants conducting privacy assessments or readiness reviews.
- Public sector officers and regulators' liaisons who interact with supervisory authorities.

- Leaders in startups and SMEs who need a practical, scalable privacy operating model.

C.4. Study Material

Topics covered:

- GDPR and Regulation (EU) 2018/1725
- ePrivacy Directive and supervisory guidance
- Lawful bases and principles
- Data subject rights
- Roles and responsibilities including the DPO
- DPIA and risk management
- Records of processing and retention
- Vendor management and international transfers including SCCs
- Breach detection, containment, and notification
- Privacy by design and default
- Governance, training, and audit

C.5. Exam Format & Difficulty Level

This is a closed book online proctored exam powered by ECVC examination platform:

- Multiple choice questions
- 50 questions per exam
- 60 minutes duration
- At least 34 questions need to be answered correctly to pass the exam
- One mark awarded for every correct answer

- No negative marking for wrong answers
- Difficulty level: Medium

C.6. Exam Outline

The 50 exam questions are distributed in thematic categories as per the below table:

Thematic Category	No. of questions	Percentage
1. Interpret EU Data Protection Law	10	20%
2. Design & Operate Privacy Controls	10	20%
3. Advise on Lawful Processing & Rights	10	20%
4. DPIA* & Incident/Breach Response	10	20%
5. DPO Role & Governance	10	20%
Total Number of Questions	50	100%

C.7. Prerequisites

There are no mandatory prerequisites. However, it is recommended to have:

- A basic understanding of the GDPR structure and key terms such as controller, processor, and lawful bases.
- Familiarity with how organisations handle data: process mapping, vendors, and records management.
- Introductory knowledge of information security controls like access control, encryption, and logging.
- Comfort reading legal or regulatory texts and summarising guidance for stakeholders.
- Awareness of EU institutions, supervisory authorities, and how guidance is published.

- Experience in a related field is helpful but not required, for example compliance, legal, security, risk, IT, or product.
- Suitable for both technical and non-technical professionals involved in data protection, compliance, or EU regulatory affairs.

D. Overview of the Certified EU AI Governance & Compliance Specialist (EUAIGO)

The Certified EU AI Governance & Compliance Specialist (EUAIGO) certification validates advanced competence in navigating the European Union's regulatory landscape for Artificial Intelligence. It equips professionals to interpret and apply the EU AI Act and related frameworks, integrating ethical, legal, and technical governance. The exam assesses understanding of conformity assessment, risk management, post-market monitoring, and organizational accountability. Through scenario-based questions, candidates demonstrate their ability to implement compliance systems aligned with EU fundamental rights and policy objectives. As part of the ECVC pathway, it follows the Certified EU Ethical AI Practitioner and Certified EU Data Protection and Privacy Officer, preparing specialists to lead responsible AI governance programs that ensure transparency, trust, and regulatory conformity across sectors. The certification corresponds to EQF Level 7, reflecting advanced specialised knowledge and applied competence in EU AI governance, compliance, and regulatory implementation.

It also supports organisations in establishing robust AI governance aligned with the EU AI Act and related regulatory obligations. It helps strengthen internal capability to manage conformity assessments, prepare and maintain compliance documentation, support post-market monitoring, and promote transparent and accountable AI practices. It also supports stronger

management of legal, ethical, and reputational risks, while improving readiness for audits, inspections, and internal or external review.

For individuals, this certification demonstrates recognised expertise in EU AI governance and compliance and supports the ability to interpret the EU AI Act, carry out risk and impact assessments, and contribute to governance policy development. It is particularly relevant for those working in compliance, legal, risk, audit, policy, and AI oversight roles, as well as for professionals seeking to strengthen their position in responsible and trustworthy AI governance within organisations.

D.1. Key Benefits

For Organisations

The Certified EU AI Governance & Compliance Specialist certification enables organisations to establish and maintain robust governance structures that align with the EU AI Act and related regulatory obligations. Certified professionals help organisations implement conformity assessments, document compliance, and manage post-market monitoring effectively. By embedding certified specialists, organisations strengthen accountability, mitigate legal and reputational risks, and foster transparent AI development practices consistent with EU fundamental rights. This certification supports continuous readiness for audits, inspections, and ethical reviews, while enhancing credibility and stakeholder trust. It demonstrates organisational maturity in responsible AI deployment and positions institutions at the forefront of EU digital compliance and innovation standards.

For Individuals

Becoming a Certified EU AI Governance & Compliance Specialist provides professionals with recognised expertise in applying EU regulatory frameworks governing artificial intelligence. It builds proficiency in interpreting the EU AI Act, conducting risk and impact assessments, and developing governance policies within organisational contexts. Certified individuals gain a competitive advantage for roles involving compliance management, AI oversight, and strategic advisory functions across public, private, and research sectors. The certification affirms mastery of complex EU digital policies, ethical AI principles, and conformity procedures. It elevates professional credibility, supports career advancement, and opens pathways to senior positions requiring regulatory knowledge and leadership in trustworthy, lawful, and human-centric AI governance.

D.2. Learning Objectives

By completing this certification, candidates will be able to:

- Interpret and apply the EU AI Act together with related EU legislation, including the GDPR, the Regulation on Data Governance, the Single Market for Digital Services, and the Data Act.
- Design and implement organisational AI governance frameworks that integrate ethical principles, human oversight, risk management, and quality management.
- Plan and execute conformity assessment procedures for high-risk AI systems, including preparation of technical documentation and the Declaration of Conformity, leading to lawful placing on the EU market.
- Establish and oversee post-market monitoring, incident reporting, corrective actions, and continuous improvement for deployed artificial intelligence systems.

- Ensure alignment of AI development and deployment with fundamental rights protected in the EU, including non-discrimination, privacy, and human dignity.
- Integrate requirements from sector-specific product legislation, including the Machinery Regulation, the Medical Devices Regulation, the In Vitro Diagnostic Medical Devices Regulation, and the General Product Safety Regulation.
- Govern data sourcing and dataset management lawfully, including provenance, licensing, copyright and database rights, transparency to affected parties, and data protection by design and by default.
- Advise senior leadership, compliance teams, and product teams on policy, controls, and documentation needed to operate trustworthy, transparent, and legally compliant AI across different sectors.
- Coordinate with notified bodies, market surveillance authorities, and data protection authorities, and prepare an organisation for audits, inspections, and supervisory requests.
- Communicate complex legal and technical requirements in clear language to stakeholders, and translate them into actionable roadmaps, metrics, and training for sustained compliance.

D.3. Target Audience

This certification is designed for professionals who are responsible for ensuring lawful, ethical, and transparent use of artificial intelligence within organisations operating under EU jurisdiction. It is particularly relevant to:

- Compliance officers and regulatory affairs managers overseeing conformity with the EU AI Act and related legislation.
- Legal advisors and policy analysts involved in digital governance, data protection, and technology regulation.

- AI project managers, product owners, and innovation leads integrating governance frameworks into system design and deployment.
- Quality management and risk management professionals implementing organisational controls and audit processes.
- Consultants, auditors, and ethics board members supporting EU compliance, certification, or conformity assessment procedures.
- Public sector officials and research coordinators guiding policy, procurement, or oversight of AI systems in regulated domains.

D.4. Study Material

Topics covered focus across the five core competence areas:

- EU AI Act interpretation
- Governance frameworks
- Conformity assessment
- Ethical and trustworthy AI
- Post-market monitoring

D.5. Exam Format & Difficulty Level

This is a closed book online proctored exam powered by ECVC examination platform:

- Multiple choice questions
- 50 questions per exam
- 60 minutes duration
- At least 36 questions need to be answered correctly to pass the exam
- One mark awarded for every correct answer
- No negative marking for wrong answers

- Difficulty level: Medium-High

D.6. Exam Outline

The 50 exam questions are distributed in thematic categories as per the below table:

Thematic Category	No. of questions	Percentage
1. EU AI Act & Core Legislation	8	16%
2. GDPR & Data Protection for AI	8	16%
3. Sectoral Product Safety Laws	5	10%
4. AI Governance Frameworks	8	16%
5. Conformity Assessment & CE ¹ Marking	5	10%
6. Post-Market Monitoring & Incident Management	5	10%
7. Responsible & Lawful AI Deployment	5	10%
8. Data Governance & IP ² Compliance	6	12%
Total Number of Questions	50	100%

¹ CE stands for "Conformité Européenne" (French) or "European Conformity" (English)

² IP stands for Intellectual Property

D.7. Prerequisites

There are no formal prerequisites. However, it is helpful to have:

- A basic understanding of European Union regulatory processes and institutional structures.
- Foundational knowledge of data protection principles, including lawful processing and data subject rights.
- General familiarity with ethical AI principles, such as transparency, accountability, and human oversight.
- Prior exposure to compliance, risk management, or governance frameworks in technology or digital policy contexts.
- Completion of the Certified EU Ethical AI Practitioner or Certified EU Data Protection and Privacy Officer certifications, or equivalent professional experience, is strongly recommended as preparation. These credentials provide essential background in ethical, legal, and data governance principles that support advanced competence in AI compliance and regulatory alignment under the European Union's Artificial Intelligence Act.

E. Overview of the Certified EU Ethical AI Practitioner (ETHAI)

The Certified EU Ethical AI Practitioner (ETHAI) certification validates a professional's ability to design, deploy, and govern artificial intelligence systems responsibly, in alignment with European Union laws and ethical standards. It demonstrates competence in applying the EU AI Act, GDPR, and the European Commission's guidelines for trustworthy and human-centric AI. The exam assesses understanding of responsible AI use, bias awareness, transparency, and human oversight throughout the AI lifecycle. Candidates learn to translate regulatory and ethical principles into practical governance measures, ensuring lawful, fair, and explainable AI systems. This certification

serves as a key pathway for professionals contributing to ethical AI adoption and compliance across both public and private EU sectors. The certification corresponds to EQF Level 5[2.1], reflecting specialised practical competence in applying ethical and legal AI principles in organisational settings.

It also supports organisations in integrating ethical and compliant AI practices across their operations. It helps strengthen alignment with the EU AI Act, GDPR, and related data governance frameworks, while supporting the development of internal policies, oversight mechanisms, and responsible AI practices. It also helps reduce compliance and reputational risks, improve transparency and accountability, and reinforce trust among regulators, partners, and the public.

For individuals, this certification demonstrates recognised expertise in ethical and lawful AI governance within the EU context and supports the ability to design, implement, and monitor AI systems in line with human rights, fairness, and transparency principles. It is particularly relevant for those working in compliance, data protection, AI governance, risk management, and related roles, as well as for professionals seeking to strengthen their credibility and progress towards leadership roles in responsible AI.

E.1. Key Benefits

For Organisations

The Certified EU Ethical AI Practitioner certification enables organisations to integrate ethical and compliant AI practices across their operations. It helps ensure that AI systems meet the obligations of the EU AI Act, GDPR, and related data governance frameworks, reducing compliance risks and reputational exposure. Certified practitioners strengthen internal governance by translating complex regulatory requirements into clear operational policies, documentation, and oversight mechanisms. Organisations benefit from improved trust, transparency, and accountability in AI deployment, reinforcing their credibility with regulators, partners, and the public. The certification also supports strategic innovation by aligning responsible AI development with

European standards, enabling participation in EU-funded projects and international collaborations.

For Individuals

The certification equips professionals with recognised expertise in ethical and lawful AI governance under the EU's evolving regulatory landscape. It validates the ability to design, implement, and monitor AI systems that uphold human rights, fairness, and transparency. Certified practitioners gain a competitive advantage in compliance, data protection, AI governance, and risk management roles. The credential enhances professional credibility across industries, including technology, finance, healthcare, and public administration. Individuals also develop the analytical and documentation skills required for conformity assessments, DPIAs, and AI risk evaluations. This certification represents a career pathway into leadership roles focused on responsible AI and regulatory alignment within European and global contexts.

E.2. Learning Objectives

By completing this certification, candidates will be able to:

- Interpret and apply the core principles of the EU Artificial Intelligence Act and related European Commission policies.
- Integrate ethical AI principles from the EU's Trustworthy AI framework into practical governance and system design.
- Assess and mitigate risks relating to bias, transparency, data governance, and human oversight across the AI lifecycle.
- Conduct and document conformity, impact, and risk assessments aligned with EU legal and ethical standards.
- Implement privacy-by-design and accountability mechanisms consistent with the GDPR and EDPB guidelines.

- Translate regulatory and ethical obligations into operational practices, policies, and controls for responsible AI development and deployment.
- Promote organisational compliance, ethical integrity, and public trust in AI innovation within the European context.

E.3. Target Audience

This certification is intended for professionals who work with or oversee AI systems within the EU context, including:

- AI project managers, data scientists, and machine learning engineers developing or implementing AI solutions.
- Compliance officers, data protection officers (DPOs), and GRC specialists ensuring legal and ethical adherence.
- Policy advisors, legal experts, and auditors involved in AI regulation, governance, and risk management.
- Public sector officials and EU institution staff responsible for digital transformation and innovation oversight.
- Professionals in regulated sectors such as finance, healthcare, education, and transport deploying AI systems.
- Consultants and advisors supporting organisations in meeting AI Act and GDPR compliance requirements.
- Researchers and academics engaged in ethical AI, human oversight, and policy development.

E.4. Study Material

Topics covered:

- EU Artificial Intelligence Act and related regulatory framework
- General Data Protection Regulation (GDPR) principles and compliance for AI

- EU Ethical Guidelines for Trustworthy AI
- Transparency and explainability requirements
- Human oversight and accountability mechanisms
- Responsible and lawful AI deployment practices

E.5. Exam Format & Difficulty Level

This is a closed book online proctored exam powered by ECVC examination platform:

- Multiple choice questions
- 50 questions per exam
- 60 minutes duration
- At least 33 questions need to be answered correctly to pass the exam (65%)
- One mark awarded for every correct answer
- No negative marking for wrong answers
- Difficulty level: Low-Medium

E.6. Exam Outline

The 50 exam questions are distributed in thematic categories as per the below table:

Thematic Category	No. of questions	Percentage
1. EU AI Act & Regulatory Framework	9	18%
2. GDPR for AI	6	12%
3. EU Ethical Guidelines for Trustworthy AI	6	12%
4. Data Governance, Fairness & Bias	9	18%

Mitigation		
5. Transparency & Explainability	6	12%
6. Human Oversight, Accountability & Governance	8	16%
7. Responsible & Lawful AI Deployment	6	12%
Total Number of Questions	50	100%

E.7. Prerequisites

There are no formal prerequisites. However, it is helpful to have:

- Basic AI concepts and lifecycle (data, training, evaluation, deployment, monitoring).
- Fundamental data protection principles and individual rights under the GDPR.
- Awareness of the EU Artificial Intelligence Act (Regulation (EU) 2024/1689) scope and key obligations.
- Introductory understanding of AI ethics, data governance, bias and fairness, transparency, and human oversight.
- Completion of the Certified EU Ethical AI Practitioner or Certified EU Data Protection and Privacy Officer certifications, or equivalent professional experience, is strongly recommended as preparation. These credentials provide essential background in ethical, legal, and data governance principles that support advanced competence in AI compliance and regulatory alignment under the European Union's Artificial Intelligence Act.
- Prior exposure to risk assessment or compliance activities (e.g., DPIA basics, documentation practices) will support effective exam preparation.

Background stability

- Open to both technical and non-technical professionals working with AI in EU contexts.

F. Overview of the Certified EU AI Data Protection & Privacy Professional (AIData)

The Certified EU AI Data Protection & Privacy Professional is an ECVC credential that validates the ability to interpret and apply EU data protection and privacy requirements in AI system contexts, with a primary focus on the GDPR, the EU AI Act, the ePrivacy Directive, official Commission AI Act guidance, and supervisory guidance on profiling and automated decision-making.

This certification is positioned as a privacy-specialist AI credential. It is not a general AI ethics certification and it is not a broad AI Act compliance certification. Its purpose is to confirm competence in assessing whether AI systems process personal data lawfully, transparently, minimally, securely, and accountably under EU privacy rules. The AI Act expressly states that EU data protection, privacy, and confidentiality of communications law continues to apply to personal data processed in connection with AI Act rights and obligations.

The scope covers authoritative EU legislation, official Commission AI Act guidance, and supervisory guidance, translated into practical day-to-day AI privacy governance. Candidates gain learning outcomes in GDPR-based AI compliance, AI privacy risk assessment, automated decision-making safeguards, lawful basis assessment, transparency, data minimisation, accuracy, retention, security, processor management, and accountability evidence.

F.1. Key Benefits

For Organisations

The Certified EU AI Data Protection & Privacy Professional helps organisations turn AI-related privacy obligations into structured, practical, and auditable compliance processes. Certified professionals identify where AI systems process personal data, assess lawful bases, review training and input data, manage profiling risks, support DPIAs, and embed privacy by design and by default, while maintaining GDPR accountability evidence. They distinguish between general AI governance and specific data protection obligations in contexts involving personal, inferred, biometric, or special category data, employee monitoring, customer scoring, behavioural advertising, automated decision-making, and cross-border data transfers. The certification improves coordination between privacy, legal, compliance, AI governance, cybersecurity, product, HR, marketing, procurement, and data science teams. It strengthens GDPR compliance, DPIA readiness, vendor due diligence, documentation quality, transparency, data subject rights handling, and regulatory preparedness while reducing legal, operational, reputational, and fundamental-rights risks linked to unsafe or opaque AI data practices.

For Individuals

The certification demonstrates verified competence in EU AI data protection and privacy practice. Candidates show the ability to interpret the GDPR, the AI Act, the ePrivacy Directive, and relevant supervisory guidance in practical AI contexts, and translate these requirements into privacy controls, DPIA inputs, governance workflows, and operational documentation. It is valuable for professionals in data protection, privacy, AI governance, legal compliance, GRC, cybersecurity, product governance, HR tech, marketing tech, fintech, healthcare, public-sector systems, procurement, audit, and consulting. It builds a practical vocabulary for working with DPOs, legal teams, AI providers, data scientists, and regulators. Certified professionals support AI privacy assessments, lawful basis analysis, transparency, profiling safeguards, biometric risk reviews, data transfers, controller–processor allocation, contract

review, and DPIA preparation, strengthening credibility in GDPR and AI Act compliance roles.

F.2. Learning Objectives

Upon successful completion of this certification, candidates will be able to:

- Interpret the GDPR in AI system contexts, including principles of lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity, confidentiality, and accountability
- Understand how the AI Act interacts with EU data protection, privacy, and confidentiality of communications rules
- Apply the AI Act definition of an AI system when assessing whether AI-related privacy risks fall within AI lifecycle governance
- Distinguish AI data protection and privacy compliance from broader AI ethics and general AI Act compliance
- Identify personal data processing activities across AI system design, training, validation, deployment, monitoring, and use
- Assess lawful bases for AI-related personal data processing, including consent, contract necessity, legal obligation, public interest, vital interests, and legitimate interests
- Recognise when AI systems involve profiling, automated decision-making, or solely automated decisions with legal or similarly significant effects
- Apply GDPR safeguards for profiling and automated decision-making, including transparency, data subject rights, meaningful human involvement, contestability, and appropriate safeguards
- Identify and assess risks linked to inferred data, derived data, behavioural data, location data, biometric data, special category data, and vulnerable data subjects

- Understand the privacy relevance of AI Act prohibited practices, including social scoring, certain profiling-based criminal risk assessment, untargeted facial image scraping, emotion recognition in workplace and education contexts, and biometric categorisation practices
- Support privacy notices and transparency information for AI systems, including information about profiling, automated decision-making, logic involved, significance, and envisaged consequences where applicable
- Operationalise data subject rights in AI contexts, including access, rectification, erasure, restriction, objection, and rights linked to automated decision-making
- Conduct and document AI-related DPIA inputs, including risk identification, necessity and proportionality analysis, safeguards, residual risks, and accountability evidence
- Embed privacy by design and by default into AI product development, procurement, testing, deployment, and monitoring
- Assess data minimisation, purpose limitation, accuracy, retention, and security controls for AI datasets and AI outputs
- Understand controller, joint controller, processor, provider, deployer, and vendor responsibilities in AI supply chains
- Review data processing agreements and standard contractual clauses where AI vendors or AI infrastructure involve processors or international personal data transfers
- Coordinate AI privacy governance with legal, security, compliance, product, procurement, HR, marketing, data science, and management teams

- Maintain auditable AI privacy documentation, including records of processing, DPIAs, vendor evidence, transfer safeguards, transparency materials, and internal decision records
- Advise stakeholders on practical AI privacy risks without treating the certification as a broad AI ethics or general AI Act compliance qualification.

F.3. Target Audience

- Current or aspiring Data Protection Officers working with AI systems
- Privacy managers, privacy analysts, and data protection professionals in EU-based or EU-facing organisations
- AI governance and compliance professionals who need deeper GDPR and privacy competence
- Legal counsel and regulatory affairs professionals advising on AI, GDPR, privacy, data processing agreements, or SCCs
- Governance, risk, compliance, audit, and internal control professionals reviewing AI privacy controls and accountability evidence
- Information security and cybersecurity professionals aligning AI security controls with GDPR requirements
- Product managers, product owners, and engineering leads building or deploying AI-enabled products
- Data scientists, machine learning teams, and AI project teams handling personal data, training data, or model outputs
- HR, recruitment, and People Operations teams using AI tools for screening, evaluation, monitoring, or workforce analytics
- Marketing, CRM, advertising, and analytics teams using AI for segmentation, targeting, profiling, or personalisation

- Healthcare, education, finance, insurance, public-sector, and security professionals involved in AI systems affecting individuals
- Procurement and vendor management teams assessing AI providers, processors, sub-processors, and data transfer risks
- Consultants supporting GDPR compliance, AI privacy readiness, DPIAs, vendor reviews, or AI system assessments
- Public-sector officers and policy professionals working with AI systems, privacy impact, automated decision-making, or digital governance
- Business leaders and decision-makers responsible for trustworthy AI deployment, privacy governance, regulatory assurance, and data protection accountability.

F.4. Study Material

Topics covered:

- GDPR principles and lawful processing in AI systems
- AI Act scope and privacy-relevant concepts
- Commission guidance on the definition of an AI system
- Prohibited AI practices with data protection relevance
- Profiling and automated individual decision-making
- ePrivacy rules
- Data subject rights
- Transparency obligations
- Data Protection Impact Assessments
- Privacy by design and by default

- AI datasets, training data, data minimisation, accuracy, retention, and security
- Controller and processor responsibilities
- AI vendor and supply-chain governance
- Standard Contractual Clauses and international transfers

F.5. Exam Format & Difficulty Level

This is a closed book online proctored exam powered by ECVC examination platform:

- Multiple choice questions
- 50 questions per exam
- 60 minutes duration
- At least 31 questions need to be answered correctly to pass the exam
- One mark awarded for every correct answer
- No negative marking for wrong answers
- Difficulty level: Medium

F.6. Exam Outline

The 50 exam questions are distributed in thematic categories as per the below table:

Thematic Category	No. of questions	Percentage
1. EU AI Act & GDPR Interface	6	12%
2. GDPR Principles & Accountability for AI	8	16%
3. AI System Definition & Scope	6	12%
4. Prohibited AI Practices & Privacy	6	12%

5. Profiling & Automated Decision-Making	8	16%
6. ePrivacy & Communications Confidentiality	6	12%
7. International Transfers & Transfer SCCs	6	12%
8. Controller–Processor Relations & SCCs	4	8%
Total Number of Questions	50	100%

F.7. Prerequisites

There are no formal prerequisites. However, it is helpful to have:

- Basic understanding of the GDPR structure and key terms such as personal data, controller, processor, data subject, lawful basis, consent, legitimate interests, DPIA, and data subject rights.
- Familiarity with AI-related concepts such as AI system, model, training data, input data, output, inference, profiling, automated decision-making, biometric data, and AI lifecycle.
- Introductory awareness of the EU AI Act and its relationship with data protection, privacy, transparency, fundamental rights, and risk-based governance.
- Familiarity with how organisations use AI tools in HR, marketing, analytics, finance, education, healthcare, public services, security, or customer operations.
- Comfort reading EU legal texts, official Commission guidance, and supervisory guidance, and translating them into practical requirements for stakeholders.

- Introductory knowledge of information security controls such as access control, encryption, logging, monitoring, vendor security, and incident response.
- Awareness of international data transfer concepts, including third-country transfers, SCCs, processors, sub-processors, and transfer safeguards.
- Experience in a related field is helpful but not required, for example privacy, compliance, legal, cybersecurity, risk, audit, product, AI governance, data science, procurement, HR, marketing, or public policy.
- Suitable for both technical and non-technical professionals involved in AI data protection, AI privacy compliance, GDPR implementation, AI system governance, DPIAs, or EU digital regulation.



LEADING THE WAY IN VOCATIONAL CERTIFICATIONS

Explore Certifications

www.ecvc.eu

Enquiries & Partnership

info@ecvc.eu

Follow ECVC for recent updates



[company/european-centre-for-vocational-certification-ecvc/](https://www.linkedin.com/company/european-centre-for-vocational-certification-ecvc/)