Next-Gen Cybercrime Investigation & Response	
GANNDALF NextGen Collaborative Cybercrime Investigation Framework	**Course title:** **Data privacy and GDPR implications in cyber investigations**
Overall aim	Creating a new landscape with respect to advanced cybercrime investigation and prevention, based on enhanced re- and up-skilling of investigators and law enforcement officers offering training on data protection law implications in cyber investigations. It emphasises a nuanced understanding of the GDPR and the Law Enforcement Directive (LED), while confronting ethical boundaries and the operational difficulties involved in managing personal data throughout cybercrime investigations.
Proficiency level	Advanced
Duration	1 day (5 hours total, divided into 6 sessions)
Target audience	LEAs, prosecutors, and judicial actors
Number of participants	Up to 20
Learning outcomes	• Distinguish between GDPR and the LED in terms of scope, legal bases, and obligations • Understand the rights of data subjects in criminal investigations and the lawful limitations that apply • Apply key principles of purpose limitation, data minimisation, proportionality, and lawfulness of processing • Evaluate real-life case law and ethical challenges in cyber investigations
Main thematic areas (topics, subtopics)	**Session 1: Legal Framework: GDPR vs. LED in Criminal Investigations (1 hour):** • Key definitions and principles (personal data, data processing, controller/processor, legal bases) • Provide an overview of the legal foundations of the GDPR and the LED, highlighting their respective scopes of application • Identify and explain the main points of convergence and divergence between the GDPR and the LED, with a particular focus on their relevance to criminal investigations **Session 2: Investigative Data Collection & Data Subject Rights (1 hour):** • Overview of data subject rights under the GDPR in the context of criminal investigations • Legal grounds and conditions for restricting these rights during investigative procedures • Balancing privacy protection with law enforcement imperatives **Session 3: Data Minimization, Retention, and International Transfers (1 hour):** • Proportionality and data minimization in practice

This work is part of the GANNDALF project. GANNDALF has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement no. 101167951

	• Retention limits and deletion obligations. Retention policies under LED vs. GDPR • Transfers to third countries: adequacy decisions, other legal requirements and operational implications **Session 4: Cross-Border Cooperation and Data Sharing Challenges (1 hour):** • MLATs, E-Evidence Regulation, and real-world cooperation • Privacy risks with global tech providers • Use of safeguards (encryption, access control, DPA oversight) • E-Evidence Regulation developments **Session 5: Key Case Law and New Considerations (30 min):** • CJEU/ECtHR decisions shaping LEA data practices • New challenges: mass surveillance, predictive policing, AI systems • **Wrap-Up, Q&A** **Session 6: GANNDALF tools - Practical demonstration (30 min)**
Cross-cutting and/or horizontal aspects	The training adopts a cross-cutting approach by integrating legal, technical, and operational perspectives on the GDPR and the LED in cybercrime investigations. It promotes awareness across disciplinary boundaries, gaining a comprehensive knowledge of the numerous elements contributing to cyber-attacks
Methods and learning strategy	Combination of presentations, real-case discussions, legal interpretation and scenario-based exercises
Learning environment	Conference room with a large screen for displaying/ online platform
Number of trainers	1
Participants' assessment/testing	yes
Course evaluation	yes
Course certification	yes

This work is part of the GANNDALF project. GANNDALF has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement no. 101167951