Università di Genova

Università di Genova | Centro Sicurezza Rischio Vulnerabilità

Sostenere la ricerca che evolve: valutazione, finanziamenti e organizzazione

La ricerca nel panorama nazionale: sicurezza e integrità della ricerca ed infrastrutture di ricerca

GdL CODAU Ricerca,
Università Cattolica del Sacro Cuore
Roma

Fabrizio Barberis
Delegato Sicurezza della Ricerca e tematiche Dual Use, Unige
16 Luglio 2026

Università di Genova

Atenei e sicurezza della ricerca

Obblighi e aspettative da MUR, export control/dual-use, FP10 e NIS2

MUR
Modello + Linee guida

→

Export control
Dual-use & UAMA

→

FP10
Horizon Europe 2028–2034

→

NIS2
Cyber-risk & incidenti

L’ateneo deve passare da adempimenti separati a una capacità stabile di governance del rischio: partner, dati, tecnologie, infrastrutture e cybersicurezza devono essere valutati insieme, prima dell’avvio delle attività.

Nota: FP10 è ancora in iter negoziale; le slide distinguono obblighi già vigenti da aspettative in consolidamento.

Fonti principali: MUR 2025; Reg. UE 2021/821; UAMA/MAECI; Commissione UE 2025; Consiglio UE 2026; D.Lgs. 138/2024 e indicazioni ACN.

Università di Genova

Mappa degli obblighi: quattro regimi, un solo sistema

Che cosa è già vincolante, che cosa è “soft law” e che cosa arriverà con FP10

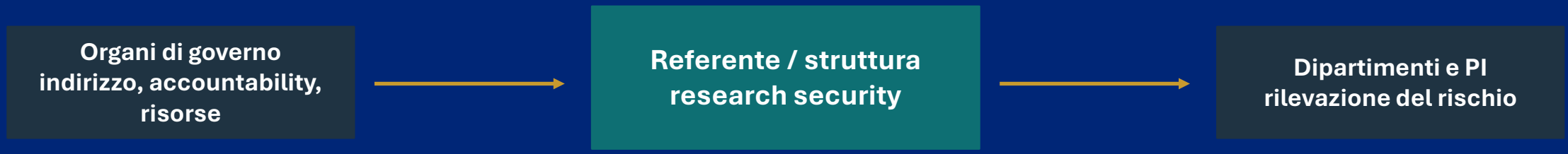
	MUR	Dual-use / export	FP10	NIS2
	Aspettativa nazionale volontaria ma strutturante	**Obbligo giuridico quando c’è esportazione/transfer**	**Regole di programma nei bandi 2028–2034**	**Obbligo cyber per soggetti in perimetro**
Governance	referente, formazione, sportello unico	ICP/export desk, tracciabilità	security self-assessment e plan	organi direttivi, risk governance
Processi	autovalutazione, due diligence	classificazione, autorizzazioni	restrizioni, controlli, mitigazione	misure, incident response, supply chain
Oggetto	partner, finanziatori, viaggi, visiting	beni, software, tecnologie, know-how	research security, dual-use by design	reti, sistemi, servizi essenziali
Evidenze	schede, escalation, misure adottate	record, licenze, end-use/end-user	documenti di proposta e gestione	audit trail, notifiche, policy

Un punto d’ingresso unico per ogni collaborazione o progetto sensibile, che smisti verso privacy, cyber, export control, IP, legale e internazionalizzazione.

Università di Genova

Linee guida MUR: cosa deve mettere in piedi un ateneo

Il modello nazionale sollecita capacità locali, raccordo con il livello nazionale e misure proporzionate



Obblighi/aspettative operative

- nominare un referente o una struttura con mandato chiaro
- creare una rete interfunzionale: ricerca, legale, TTO, privacy, IT/cyber, internazionalizzazione, HR, facility
- pubblicare pagine web e canali interni come sportello unico
- formare ricercatori, dottorandi, visiting, project manager e personale tecnico-amministrativo
- definire procedure di escalation e supporto per casi critici

Evidenze da produrre

- policy e linee operative approvate
- scheda di autovalutazione e registro delle decisioni
- piani di mitigazione e responsabilità assegnate
- registro formazione, briefing viaggi/visiting, accessi e incidenti
- report periodico agli organi di governo

La libertà accademica resta il punto di partenza; la responsabilità istituzionale è la condizione per proteggerla.

Università di Genova

Export control e dual-use: l’obbligo scatta anche nella ricerca

Non riguarda solo spedizioni fisiche: include software, tecnologia e assistenza tecnica

Ambito da verificare

Beni	Software	Tecnologia	Assistenza tecnica
strumenti, componenti, materiali	codice, modelli, firmware	dati tecnici, disegni, know-how	formazione, supporto, accesso remoto

Adempimenti essenziali per l’ateneo

- classificare beni, software e tecnologie rispetto agli allegati dual-use e alle clausole catch-all
- identificare destinazione, end-user, end-use e finanziatori
- verificare sanzioni, embarghi e restrizioni Paese/soggetto
- richiedere autorizzazioni quando necessario tramite canali competenti
- mantenere un Internal Compliance Programme per la ricerca dual-use

Red flags tipiche in università

- training tecnico a partner extra-UE su tecnologia sensibile
- accesso remoto a server contenenti codice o dati tecnici
- spedizione di prototipo, sensore, drone, materiale o campione
- visiting in laboratorio con accesso a strumentazione avanzata
- clausole che impongono segretezza anomala o uso non chiaro

Quando non è chiaro se sia “solo scienza”, trattarlo come caso da classificare: la mancata valutazione è il vero rischio.

Università di Genova

NIS2: la cyber-security diventa governance del rischio

Per gli atenei in perimetro NIS: misure, responsabilità e notifiche; per gli altri: baseline di resilienza

Governance
organi direttivi informati e responsabili

Risk management
misure tecniche, organizzative e supply chain

Incidenti
processo CSIRT, notifiche, evidenze

Continuità
backup, crisi, recovery, audit

Che cosa cambia per la sicurezza della ricerca

- gli asset di ricerca entrano nel risk register: HPC, strumentazioni, piattaforme dati, repository, laboratori
- gli accessi di visiting, partner e fornitori devono essere governati con identità, autorizzazioni e logging
- gli incidenti cyber che impattano attività o servizi devono essere gestiti e notificati secondo procedure definite
- il rischio supply chain riguarda anche cloud, strumenti scientifici, manutentori, consorzi e gestori di infrastrutture

Integrazione necessaria

NIS2 non è solo “tema IT”: deve essere collegata a due diligence partner, export control, protezione dei dati, continuità delle infrastrutture e gestione dei progetti.

Nota: l’applicabilità concreta dipende dalla classificazione del soggetto e dai servizi svolti. Anche fuori perimetro, le misure NIS2 sono una baseline utile per research security.

Università di Genova

FP10: cosa preparare prima che diventi requisito di bando

Il Consiglio UE ha già inserito research security, restrizioni proporzionate e dual-use by design

Security self-assessment nel dossier di proposta	**Initial security management plan misure e responsabilità**	**Restriction by risk partner, controllo, Paese, risultati**	**Dual-use by design Pillar II e EIC**

Impatti pratici su proposta e consorzio

- screening anticipato di partner, soggetti controllanti e Paesi di stabilimento
- descrizione di accessi, dati, asset e risultati da proteggere
- piano di mitigazione integrato con IP, dati, cyber ed export control
- controllo di cambiamenti nel consorzio e nei finanziatori durante il progetto

Punti ancora aperti nel negoziato

- budget e ripartizioni definitive
- confine tra dual-use e ricerca esclusivamente militare
- dettaglio delle condizioni di partecipazione dei Paesi terzi
- rapporto operativo fra Horizon Europe, EIC ed ECF

Per vincere bandi sensibili servirà dimostrare “security readiness” già in proposal, non solo adeguarsi dopo il grant agreement.

Council of the EU | Press release | 26 June 2026 09:59

MFF 2028-2034: Council agrees its position on Horizon Europe, the new and ambitious framework programme for research and innovation

The Council has reached an agreement on its partial negotiating position on the regulation and the specific programme of the Horizon Europe, the tenth EU framework programme for research and innovation. Horizon Europe is a key element of the next multiannual financial framework (MFF), the EU's seven-year spending plan. It is designed to drive scientific excellence, boost economic competitiveness, and tackle global societal challenges. Besides the proposed substantial budget increase by the Commission, the agreed Council position for Horizon Europe foresees a tight link with the EU's competitiveness instrument in the next MFF, the European Competitiveness Fund (ECF), to facilitate a seamless investment support journey.

Università di Genova

Modello integrato: un intake, cinque valutazioni coordinate

Come evitare frammentazione fra MUR, dual-use, NIS2, privacy e FP10

Solo i casi medi/alti passano al tavolo interfunzionale; i casi bassi seguono check automatici e template standard. Questo rende il sistema sostenibile.

Università di Genova

Checklist per il decisore universitario

Domande da portare in CdA/Senato/Direzione Generale

Governance	Abbiamo un referente con mandato, escalation e risorse?
Processo	Ogni collaborazione sensibile entra da un punto unico?
Partner	Conosciamo proprietà, controllo, finanziatori e finalità d'uso?
Tecnologia	Classifichiamo dati, software, prototipi e know-how?
Export	Sappiamo quando serve autorizzazione o parere specialistico?
Cyber/NIS2	Gli asset di ricerca sono nel risk register e nel piano incidenti?
Infrastrutture	Gestiamo visiting, accessi, logging, facility e supply chain?
FP10	Siamo pronti a produrre security self-assessment e security plan?

Approvare una funzione trasversale di research security integrata con export control e cyber-risk, con pilota immediato sulle infrastrutture e sui progetti internazionali sensibili.

Centro Sicurezza Rischio Vulnerabilità

Università di Genova

Università di Genova

Grazie

fabrizio.barberis@unige.it