Università di Genova

Politica - Sicurezza dei dati

Documento: GV_PO-01l - Versione 2.0 – 10 settembre 2026

Sommario

1 – Principi generali
2 – Impegni degli Organi di Amministrazione e direttivi NIS2
3 – Classificazione e protezione commisurata alla criticità dei dati
4 – Protezione dei dati a riposo e in transito
5 – Backup, disponibilità e conservazione dei dati
6 – Incidenti e data breach
7 – Documentazione ed evidenze
8 – Revisione e approvazione

Università di Genova

1 – Principi generali

L'Università degli Studi di Genova (di seguito "Ateneo" o "UniGe") riconosce che la protezione dei dati costituisce una misura essenziale per garantire la riservatezza, l'integrità e la disponibilità delle informazioni trattate nell'ambito dei sistemi informativi e di rete. A tal fine, adotta misure organizzative e tecniche proporzionate al rischio per proteggere i dati durante la memorizzazione, la trasmissione, l'utilizzo e il ripristino, tenendo conto della criticità delle informazioni trattate e dei sistemi che le elaborano.

La presente politica si coordina con il Regolamento (UE) 2016/679 (GDPR), con il D.lgs. 30 giugno 2003, n. 196, come modificato dal D.lgs. 10 agosto 2018, n. 101, con il Regolamento dell'Università degli Studi di Genova in materia di trattamento dei dati personali e con il Regolamento di Ateneo per la sicurezza informatica. Essa si applica ai dati personali e non personali trattati nell'ambito delle attività istituzionali di amministrazione, didattica, ricerca e terza missione.

2 – Impegni degli Organi di Amministrazione e Direttivi NIS2

Gli Organi di Amministrazione e Direttivi NIS2 adottano indirizzi strategici e misure organizzative finalizzate a supportare i seguenti obiettivi:

- assicurare l'adozione di misure idonee a proteggere i dati a riposo e in transito, in coerenza con gli esiti della valutazione del rischio;
- garantire che, fatte salve motivate e documentate ragioni normative o tecniche, siano utilizzati protocolli e algoritmi di cifratura allo stato dell'arte e considerati sicuri nei casi previsti;
- promuovere adeguate misure di protezione dei dispositivi portatili e dei supporti removibili;
- assicurare l'effettuazione periodica dei backup dei dati e delle configurazioni in funzione delle esigenze di continuità operativa e di ripristino in caso di disastro;
- garantire che, per almeno i sistemi informativi e di rete rilevanti, sia sviluppata una strategia di implementazione di un sistema per il backup fuori linea (o tecnologia con livelli di sicurezza equivalente) per i casi applicabili, e fatte salve le diverse strategie di data governance previste nei sistemi cloud, quali ad es. la creazione di archivi di backup presso un ulteriore cloud service provider certificato rispetto a quello primariamente utilizzato. Le presenti misure sono subordinate alle relative disponibilità di bilancio;
- assicurare il coordinamento tra governo della cybersicurezza e protezione dei dati personali, consultando il Responsabile della protezione dei dati (DPO) nei casi previsti dal GDRP e dal Regolamento di Ateneo per la sicurezza informatica;
- garantire che la classificazione dei dati e l'individuazione delle misure siano integrate nel censimento e nella caratterizzazione degli asset ICT, in coerenza con la delibera del Consiglio di amministrazione n. 275 del 26 novembre 2025 e s.m.i. e con la relativa procedura di mappatura;

- assicurare che fornitori e altri responsabili esterni del trattamento offrano garanzie adeguate e siano disciplinati da atti conformi all'art. 28 GDPR, con obblighi di sicurezza, riservatezza, collaborazione e tempestiva segnalazione degli incidenti.

3 – Classificazione e protezione commisurata alla criticità dei dati

La protezione dei dati è commisurata al livello di criticità attribuito nel censimento dei sistemi informativi e di rete. La classificazione considera la natura personale o non personale dei dati e l'impatto che perdita di disponibilità, autenticità, integrità o riservatezza può produrre sulle persone interessate e sull'assolvimento dei compiti istituzionali dell'Ateneo. Per ciascun sistema viene attribuito un livello di criticità del dato presente, corrispondente al livello più elevato tra i dati in esso inseriti (criterio del "caso peggiore").

In prima applicazione si identificano alcune classi di criticità crescente dei dati che potranno essere aggiornate anche in base all'evoluzione del contesto della cybersicurezza:

- Livello 1 – dati personali già pubblicati o comunque a criticità contenuta (ad esempio curriculum vitae già pubblicati), ferma la verifica della base giuridica e delle finalità del trattamento;
- Livello 2 – dati non personali a diffusione controllata, quali materiali didattici destinati agli studenti iscritti, e dati personali ordinari, quali codice fiscale o altro identificativo di personale o studenti;
- Livello 3 – dati personali o non personali con rilevanza strategica o confidenziale, quali dati di ricerca e strategie dell'Ateneo, nonché categorie particolari di dati che, nel contesto concreto, richiedano protezione rafforzata;
- Livello 4 – dati personali a criticità elevata, inclusi dati sanitari, genetici, biometrici destinati a identificare in modo univoco una persona e dati relativi a condanne penali e reati, nonché ulteriori dati la cui compromissione possa determinare un impatto significativo sulle attività istituzionali dell'Ateneo.

La classificazione degli asset in rapporto al livello di criticità dei dati è validata dai responsabili della struttura e, per i contesti di ricerca, anche dai responsabili scientifici, con il supporto dei referenti tecnici e degli Amministratori di sistema. Essa è aggiornata quando cambiano dati, finalità, tecnologie, destinatari, esposizione o dipendenze del sistema. Con un approccio commisurato al livello di criticità dei dati sono adottate, secondo l'analisi del rischio, a titolo esemplificato e non esaustivo, misure rafforzate quali segregazione degli accessi, autenticazione forte, cifratura, pseudonimizzazione, ove appropriata, tracciamento degli accessi amministrativi, monitoraggio, copie di sicurezza protette e verifiche periodiche.

Le suddette misure vanno comunque adattate all'evoluzione tecnologica, che più richiedere l'introduzione di ulteriori misure e compatibilmente con le risorse di bilancio allocate.

Quando un trattamento può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, è svolta la valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35 GDPR, con consultazione del DPO.

4 – Protezione dei dati a riposo e in transito

Per almeno i sistemi informativi e di rete rilevanti, e, nello specifico, per i dati rilevanti come descritti al paragrafo precedente, in accordo con gli esiti della valutazione del rischio, l'Ateneo adotta misure idonee a proteggere i dati sia durante la memorizzazione sia durante la trasmissione da e verso l'esterno dell'organizzazione, mediante l'utilizzo di protocolli e algoritmi di cifratura allo stato dell'arte e considerati sicuri, fatte salve motivate e documentate ragioni normative o tecniche. In tale ambito, i dati memorizzati sui dispositivi portatili, inclusi laptop, smartphone e tablet, nonché sui supporti removibili, sono protetti con misure adeguate al rischio e, ove previsto, cifrati; inoltre, fatte salve motivate e documentate ragioni normative o tecniche, è disabilitata l'auto esecuzione dei supporti rimovibili ed è effettuata la loro scansione prima dell'utilizzo nei sistemi informativi e di rete.

L'adeguatezza delle misure di cifratura è valutata e riesaminata periodicamente in funzione della criticità dei dati, delle modalità e del contesto del trattamento, dell'evoluzione tecnologica e degli esiti della valutazione del rischio. Le modalità applicative e gli eventuali criteri tecnici di dettaglio sono definiti nella documentazione attuativa dell'Ateneo.

Per i dispositivi d'ufficio (es. desktop) o portatili e/o di produttività individuale, anche al fine di mitigare i rischi di perdita o divulgazione dei dati derivanti da smarrimento o furto, l'Ateneo adotta progressivamente, quale configurazione predefinita, la cifratura degli archivi e dei supporti di memorizzazione.

La gestione dei dispositivi di cui al periodo precedente è attuata a livello standard, ove tecnicamente possibile, e fatti salvi aspetti di incompatibilità presenti in sistemi di ricerca e sviluppo, mediante sistemi centralizzati e automatizzati di gestione degli endpoint quali MDM – Mobile Device Management, XDR – Extended Detection and Response. Eventuali diverse configurazioni devono essere concordate con l'Area ICT.

5 – Backup, disponibilità e conservazione dei dati

In accordo con le esigenze di continuità operativa e di ripristino in caso di disastro individuate nei piani adottati dall'organizzazione, sono effettuati periodicamente i backup dei dati e delle configurazioni. Per almeno i sistemi informativi e di rete rilevanti si adattano idonee strategie di backup, commisurate ai livelli di servizio da garantire per i diversi sistemi e alle tipologie di dati in essi gestiti.

Frequenza, retention, isolamento, cifratura e prove di ripristino dei backup sono definite in funzione della criticità dei dati e degli obiettivi di continuità. Le copie sono assoggettate a controlli di accesso e cancellazione coerenti con il ciclo di vita del dato. Per i dati personali, i tempi di conservazione sono determinati in base alle finalità, agli obblighi normativi e al principio di limitazione della conservazione; la presenza nei backup non deve determinare una conservazione indefinita e le procedure di ripristino devono evitare la reintroduzione non necessaria di dati già cancellati o rettificati.

6 – Incidenti e data breach

Nel trattamento dei dati personali e non personali, comunque rilevanti, si applicano la procedura di gestione degli incidenti approvata ai sensi dell'art. 25 D.lgs 138/2024 con delibera del 22 dicembre 2025 e s.m.i. e la procedura di segnalazione del data breach, ove riscontrata, prevista ai sensi del GDPR e del Regolamento privacy di Ateneo. Le procedure si conformano inoltre alle tempistiche di notifica alle Autorità previste dalle relative normative NIS2 e GDPR.

7 – Documentazione ed evidenze

Le attività svolte ai fini della sicurezza dei dati sono supportate da adeguata documentazione ed evidenze. Tale documentazione è conservata secondo le modalità definite dall'organizzazione, in modo da garantirne disponibilità, integrità e tracciabilità.

Le evidenze comprendono, per quanto applicabile: classificazione dei dati e associazione agli asset censiti; valutazione del rischio e d'impatto; esiti dei backup e delle prove di ripristino; misure compensative; accordi con responsabili esterni al trattamento; registrazioni degli incidenti e delle violazioni di dati personali. La documentazione è accessibile ai soli soggetti autorizzati ed è conservata per periodi coerenti con le finalità di controllo e con la normativa applicabile.

8 – Revisione e approvazione

La presente politica è approvata dagli Organi di Amministrazione e direttivi NIS2 ed entra in vigore alla data di adozione. La revisione avviene con cadenza programmata, a seguito di cambiamenti organizzativi, tecnologici o normativi significativi, o in seguito a incidenti di sicurezza.