

Protezione dei dati personali

Il 25 maggio 2018 è entrato in vigore nella Unione Europea il **Regolamento generale sulla protezione dei dati (GDPR)** che, per meglio tutelare il diritto dei propri cittadini alla protezione dei dati personali, evolve le legislazioni preesistenti degli stati membri.

La legislazione precedente all'entrata in vigore del GDPR era già particolarmente stringente per quanto riguarda il trattamento dei dati sensibili; a tal proposito, Cineca da diversi anni mantiene la certificazione internazionale ISO-27001 del proprio sistema di gestione della sicurezza delle informazioni. Tuttavia l'adeguamento al GDPR ha richiesto a Cineca adeguamenti al fine di mantenere la conformità con la nuova normativa, in riferimento a:

- Controllo degli accessi;
- Gestione degli atti di nomina;
- Sicurezza dei dati;
- Gestione delle possibili violazioni dei dati (data breach);
- Valutazione d'impatto;
- Minimizzazione del trattamento;
- Diritti dell'interessato;
- Responsabile della Protezione dei dati (DPO).

CONTROLLO DEGLI ACCESSI

La profilazione degli utenti dei sistemi informativi della rete Cineca soddisfa i requisiti della norma "ISO27001:2013" sulla gestione della sicurezza delle informazioni. La gestione del controllo degli accessi è dettagliata in opportune procedure e istruzioni operative, con l'obiettivo di:

- prevenire accessi di utenti non autorizzati alle risorse e servizi in rete;
- controllare l'allocazione dei diritti di accesso ai sistemi e i servizi in rete;
- definire le regole per gestire tutto il ciclo di vita di un account: dalla registrazione iniziale del nuovo utente, alla cancellazione finale dell'utente;
- definire le responsabilità dell'operatore e le regole comportamentali per prevenire accessi logici di personale non autorizzato.

ATTI DI NOMINA A RESPONSABILI DEL TRATTAMENTO

Per tutti i trattamenti operati è stata formalizzata la nomina del Cineca quale Responsabile del trattamento.

Analogamente, Cineca ha provveduto a predisporre e a far sottoscrivere gli atti di nomina per regolare il trattamento dei dati personali da parte dei propri fornitori (sub responsabili).

SICUREZZA DEI DATI

Il GDPR prescrive l'obbligo di mettere in atto misure adeguate per assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento.

Garantire la **riservatezza** significa evitare che vi sia un accesso a dati personali da parte di persone non autorizzate. Cineca gestisce il controllo degli accessi con questo preciso obiettivo, e per prevenire accessi non autorizzati con scopi malevoli, pianifica periodicamente test di vulnerabilità dei propri sistemi informatici.

Cineca predispone misure idonee per evitare l'alterazione, accidentale o dolosa, dei dati personali (**integrità**) e per assicurare l'accesso ai dati alle persone autorizzate (**disponibilità**). Se per qualsiasi motivo i due requisiti di integrità e disponibilità venissero temporaneamente a mancare, Cineca si impegna a ripristinare una situazione corretta nel minor tempo possibile (**resilienza**).

Inoltre in Cineca è attivo un sistema di backup di tutti i dati e di Disaster Recovery per i servizi più critici.

VIOLAZIONE DEI DATI

Il GDPR riserva una attenzione particolare alla gestione della violazione dei dati personali (il cosiddetto “**data breach**”), descrivendo con precisione le azioni da svolgere nel momento in cui un Titolare od un Responsabile del Trattamento vengono a conoscenza di una violazione.

Cineca ha predisposto una istruzione operativa per il trattamento dei sospetti data breach, coerente con quanto richiesto dal GDPR, con lo scopo di:

- minimizzare il danno derivante da incidenti che coinvolgono la sicurezza di dati personali
- definire le modalità operative per la gestione di data breach al fine di garantire una risposta immediata ed efficace;
- tenere sotto controllo tali eventi ed imparare da essi;
- documentare, tramite registrazioni formali, tutte le azioni intraprese per rispondere al data breach
- stabilire le modalità operative e le responsabilità nelle comunicazioni relative a violazioni di dati personali (data breach), di cui Cineca è Titolare o Responsabile, nel rispetto della normativa.

VALUTAZIONE D’IMPATTO

Cineca si impegna, in qualità di Titolare, a svolgere le valutazioni d’impatto sulla protezione dei dati (DPIA) per quanto riguarda i nuovi trattamenti, o per i trattamenti preesistenti se configurino una possibile variazione del rischio in seguito ad una revisione.

Laddove invece agisca in qualità di Responsabile, Cineca assume l’impegno a coadiuvare il Titolare in tali valutazioni.

MINIMIZZAZIONE DEL TRATTAMENTO

Il GDPR, riprendendo il concetto di minimizzazione del trattamento dei dati personali, introduce l’obbligo di adottare misure adeguate sia in fase di progettazione (**protection by design**) che per impostazione predefinita (**protection by default**) allo scopo di realizzare l’applicazione di tale principio.

Per ottenere la minimizzazione del trattamento a livello di progettazione vengono applicate misure quali la pseudonimizzazione, la separazione degli archivi che riguardano i dati personali dai dati sensibili, collegando i due archivi tramite codici anonimi, ed applicando algoritmi di cifratura adeguati nello scambio dei dati in rete.

La minimizzazione del trattamento a livello di impostazione predefinita viene ottenuta individuando quali sono i dati personali strettamente necessari al servizio in accordo col Titolare, e codificando tali informazioni nel registro dei trattamenti, che il GDPR prevede sia redatto sia dal Titolare che dal Responsabile.

Infine un altro aspetto funzionale alla sicurezza dei dati indicato dal Regolamento è che l’accesso ai dati personali sia autorizzato per il numero di persone strettamente necessario allo svolgimento delle operazioni connesse al trattamento. La definizione di profili individuali consente di concedere l’accesso ai dati, alle sole persone autorizzate.

DIRITTI DELL’INTERESSATO

Cineca, in qualità di Titolare del Trattamento, deve provvedere alla predisposizione delle **informative** sul trattamento dei dati personali e, quando necessario, alla raccolta del consenso, nel caso la base giuridica del trattamento sia il consenso.

Si impegna inoltre a coadiuvare il Titolare in questa attività con riguardo ai trattamenti ove agisce in veste di Responsabile.

All’interessato il GDPR conferma ed estende il **diritto di ottenere dal Titolare una serie di informazioni** che riguardano il trattamento dei propri dati personali, e a richiedere al Titolare copia dei dati personali che lo riguardano, la loro **modifica o limitazione**, od anche la loro **cancellazione**, ove non in contrasto con altre norme cogenti.

Le procedure di Cineca sono state adeguate per consentire di rispondere alle esigenze dell’interessato, nei casi previsti dalla legge. Per rispondere a tali richieste, Cineca ha attivato un punto di riferimento costituito dalla email:

privacy@cineca.it

RESPONSABILE DELLA PROTEZIONE DEI DATI (DPO)

In ottemperanza al dettato del GDPR, Cineca ha nominato un responsabile della protezione dei dati (**DPO**) al proprio interno), avente i seguenti compiti:

- a) informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti in merito agli obblighi derivanti dalle norme vigenti in tema di protezione dei dati personali;
- b) sorvegliare l'osservanza dalle norme vigenti e dei regolamenti aziendali in tema di protezione dei dati personali;
- c) fornire valutazioni d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento;
- d) cooperare con l'autorità di controllo;
- e) fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento.