SSM
Scuola Superiore Meridionale

POLITICA PER LA PROTEZIONE DEI DATI

Regolamento UE 2016/679 – GDPR

Politica per la protezione dei dati personali, al fine di tutelare i diritti e le libertà fondamentali delle persone fisiche

INDICE

1. SCOPO

Scopo del presente documento è quello di descrivere i principi generali di sicurezza ed obblighi di riservatezza delle informazioni e dei dati personali definiti dal Titolare del trattamento che **la Scuola Superiore Meridionale** (di seguito anche "S.S.M.") garantisce ed assicura a tutti i soggetti coinvolti nell'ambito del trattamento dei dati, al fine di sviluppare un efficiente e sicuro sistema di gestione delle procedure e dei processi per la sicurezza dei dati personali nel rispetto dei diritti e le libertà fondamentali delle persone, in ottemperanza al Regolamento Europeo 2016/679, d'ora in avanti GDPR.

2. DESCRIZIONE

Obiettivi perseguiti

La Scuola Superiore Meridionale intende perseguire obiettivi di sicurezza delle informazioni, dei dati personali, della struttura tecnologica, fisica, logica ed organizzativa e della loro gestione. Questo significa raggiungere e mantenere un sistema di gestione sicura delle informazioni attraverso il rispetto dei principi previsti dagli articoli 5 e 6 del GDPR;

- Liceità, correttezza, trasparenza;
- Garanzia rispetto alla gestione e raccolta dei dati per le sole finalità contrattuali, determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità. Tali garanzie sono applicate e verificate anche a cascata nei confronti degli eventuali subfornitori;
- Adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (principio di "minimizzazione dei dati");
- Esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o

rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»);

- Conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati;

- Trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche ed organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentale: "principio di integrità e riservatezza";

- Assicurare che i dati personali siano accessibili solamente ai soggetti e/o alle categorie degli stessi debitamente autorizzati;

- Salvaguardare la consistenza dell'informazione da modifiche non autorizzate;
- Assicurare che gli utenti autorizzati abbiano accesso alle informazioni e agli elementi architetturali associati in riferimento ai ruoli e mansioni ricoperti;

- Assicurare che la gestione dei dati avvenga sempre attraverso processi e strumenti sicuri e testati;

- Garantire l'affidabilità dei canali di provenienza delle informazioni;

- Garantire la protezione ed il controllo dei dati personali.

Formazione
Considerato che il GDPR, a mente dell'articolo 29, prevede che tutte le persone, addetti, incaricati, sotto l'autorità del titolare o del responsabile del trattamento, per l'effettuazione delle operazioni di trattamento dei dati debbano essere debitamente istruiti e, quindi, formati sui compiti che gli vengono assegnati, **La Scuola Superiore Meridionale** ha redatto un piano interaziendale di formazione sulla base dell'erogazione dei servizi, dei ruoli e mansioni interne, dell'attività esercitata, degli specifici trattamenti dati ed i rischi connessi.

La formazione è pensata e realizzata per le mansioni ed i ruoli ricoperti dal personale dipendente e ed ha le seguenti caratteristiche:

a) Specifica - corrispondente alla tipologia di mansione/ruolo svolto;
b) Appropriata - in relazione alla tipologia dei trattamenti dati realizzati;
c) Permanente - deve prevedere una programmazione temporale ed un aggiornamento periodico in particolare per eventuali nuovi assunti;
d) Documentata - il suo svolgimento ed i successivi aggiornamenti devono risultare da registri, attestati o altre forme che ne diano evidenza;
e) Efficace – deve essere verificata periodicamente la comprensione generale.

Nei confronti dei nostri fornitori:
Tali principi e garanzie sono verificate al momento della scelta di ogni nostro fornitore. Viene inoltre monitorato sistematicamente lo stato di implementazione di tali garanzie.

3. AMBITO DI APPLICAZIONE

La politica per la protezione dei dati personali si applica a tutto il personale interno ed alle terze parti che collaborano alla gestione delle informazioni nonché a tutti i processi e risorse coinvolte nella progettazione, realizzazione, avviamento ed erogazione continuativa nell'ambito dei servizi.

4. POLITICA PER LA SICUREZZA DELLE INFORMAZIONI

La S.S.M., prima di trattare i dati personali, verifica la finalità e la base giuridica su cui si fonda ogni trattamento effettuato, anche al fine di rendere adeguata informativa ai soggetti interessati, come previsto dagli artt. 13 e 14 del GDPR;

- Sono state predisposte, pertanto, le informative da mostrare agli interessati nel rispetto di tutti gli elementi indicati agli artt. 13 e 14 del GDPR. In particolare, gli interessati vengono messi a conoscenza dei diritti che il Regolamento riconosce loro (diritto di accesso, diritto all'oblio, diritto di rettifica, diritto di limitazione e di opposizione al trattamento, diritto alla portabilità dei dati);

- E' stato predisposto, inoltre, il registro delle attività di trattamento dei dati personali ai sensi dell'art. 30 del GDPR, che verrà man mano implementato.

- E' stata prevista anche una procedura da adottare in caso di eventuali violazioni dei dati (c.d. Data Breach di cui agli articoli 33 e 34 del GDPR), ad esempio al verificarsi di una divulgazione (intenzionale o meno), della distruzione, della perdita, della modifica o dell'accesso non autorizzato ai dati personali oggetto di trattamento.
Il GDPR, infatti, prevede degli specifici adempimenti nel caso in cui si verifichi una violazione di tal genere, a causa, ad esempio, di un attacco informatico, di un accesso abusivo o di un incidente. In questi casi il GDPR impone al Titolare del trattamento, a mente dell'art. 33, l'obbligo di comunicare all'autorità di controllo l'avvenuta violazione entro 72 ore (o comunque senza ritardo). Nel caso in cui la violazione verificatasi faccia presumere che vi sia anche un elevato e attuale pericolo per i diritti e le libertà degli interessati, anche questi ultimi dovranno essere direttamente informati senza ritardo di quanto successo;

- La S.S.M., inoltre, in ossequio a quanto disposto dall'art. 35 del GDPR, e con espresso riferimento a quei trattamenti che, in considerazione della natura, dell'oggetto, del conteso e della finalità presentino un rischio elevato per i diritti e le libertà delle persone fisiche, ha provveduto ad effettuare una valutazione d'impatto sulla protezione dei dati.
A tal uopo si precisa che il GDPR non sancisce un vero e proprio obbligo di svolgimento della valutazione d'impatto, ma si ricorda che il Regolamento prevede un generale obbligo, in capo al Titolare del trattamento, di attuare le misure idonee al fine di gestire adeguatamente i rischi per i diritti e le libertà degli interessati che possono derivare dal trattamento dei loro dati. Sarà opportuno procedere, quindi, all'effettuazione della valutazione d'impatto anche quando sul Titolare non incombe l'obbligo normativo in tale senso.

ISTRUZIONI PER I SOGGETTI INTERNI E/O ESTERNI CHE SI INTERFACCIANO CON LA SCUOLA SUPERIORE MERIDIONALE

Particolare importanza viene attribuita alle procedure del Sistema di Gestione per la Protezione dei dati personali, indicate nelle istruzioni e formazione che dovranno essere fornite al personale dipendente della S.S.M. ed alle quali vi è l'obbligo di attenersi scrupolosamente.

Periodicamente o all'occorrenza dovrà essere svolto un riesame per la verifica dell'efficienza e dell'efficacia, nonché dell'adeguatezza delle misure tecniche/organizzative applicate, nel rispetto ed al fine ultimo della protezione dei dati, diritti e libertà fondamentali delle persone.

Napoli, 12/06/2023

Per approvazione

Firmato digitalmente da: FISCIANO Ferdinando
Organizzazione: Universita' di Napoli Federico II
Data: 15/06/2023 13:19:02

Firmato digitalmente da: De Vivo Arturo
Organizzazione: Università degli Studi di Napoli Federico II
Data: 15/06/2023 13:20:32