Ministero dell'Istruzione e del Merito - Ufficio Scolastico Regionale per la Lombardia
LICEO STATALE "GALILEO GALILEI"
Scientifico-Classico-Linguistico-Sportivo
Viale Gorizia, 16 - 20025 Legnano (MI) Tel. 0331/542402 - 549398
Email: mips13000n@istruzione.it - segreteria@lscgalilei.it - mips13000n@pec.istruzione.it
Sito web https://www.liceogalileilegnano.edu.it
Cod. Mecc.: MIPS13000N - C.F. 84004510156

REGOLAMENTO PER IL RIUTILIZZO E LO SMALTIMENTO DI APPARECCHIATURE ELETTRONICHE E SUPPORTI DI MEMORIZZAZIONE

INDICE

Art. 1 - Definizioni

Di seguito si riportano alcune definizioni rilevanti ai fini del presente regolamento; per le altre definizioni si rimanda all'art. 4 del Regolamento UE 2016/679 – GDPR.

Ai fini del presente regolamento s'intende per:

1) **«dato personale»**: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

2) **«trattamento»**: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

3) **«limitazione di trattamento»**: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;

4) **«profilazione»**: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

5) **«pseudonimizzazione»**: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;

6) **«archivio»**: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;

7) **«titolare del trattamento»**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

8) **«responsabile del trattamento»**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

9) **«destinatario»**: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;
10) **«terzo»**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;

11) **«consenso dell'interessato»**: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante

dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;

12) **«violazione dei dati personali»**: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;

13) **«dati genetici»**: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;

14) **«dati biometrici»**: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;

15) **«dati relativi alla salute»**: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

16) **«stabilimento principale»**:

a) per quanto riguarda un titolare del trattamento con stabilimenti in più di uno Stato membro, il luogo della sua amministrazione centrale nell'Unione, salvo che le decisioni sulle finalità e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del titolare del trattamento nell'Unione e che quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni, nel qual caso lo stabilimento che ha adottato siffatte decisioni è considerato essere lo stabilimento principale;

b) con riferimento a un responsabile del trattamento con stabilimenti in più di uno Stato membro, il luogo in cui ha sede la sua amministrazione centrale nell'Unione o, se il responsabile del trattamento non ha un'amministrazione centrale nell'Unione, lo stabilimento del responsabile del trattamento nell'Unione in cui sono condotte le principali attività di trattamento nel contesto delle attività di uno stabilimento del responsabile del trattamento nella misura in cui tale responsabile è soggetto a obblighi specifici ai sensi del presente regolamento;

17) **«rappresentante»**: la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento;

18) **«impresa»**: la persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le società di persone o le associazioni che esercitano regolarmente un'attività economica;

19) **«gruppo imprenditoriale»**: un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate;

20) **«norme vincolanti d'impresa»**: le politiche in materia di protezione dei dati personali applicate da un titolare del trattamento o responsabile del trattamento stabilito nel territorio di uno Stato membro al trasferimento o al complesso di trasferimenti di dati personali a un titolare del trattamento o responsabile del trattamento in uno o più paesi terzi, nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune;

21) **«autorità di controllo»**: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51;

22) **«autorità di controllo interessata»**: un'autorità di controllo interessata dal trattamento di dati personali in quanto:

a) il titolare del trattamento o il responsabile del trattamento è stabilito sul territorio dello Stato membro di tale autorità di controllo;

b) gli interessati che risiedono nello Stato membro dell'autorità di controllo sono o sono probabilmente influenzati in modo sostanziale dal trattamento; oppure

c) un reclamo è stato proposto a tale autorità di controllo;

23) **«trattamento transfrontaliero»**:

a) trattamento di dati personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un titolare del trattamento o responsabile del trattamento nell'Unione ove il titolare del trattamento o il responsabile del trattamento siano stabiliti in più di uno Stato membro; oppure

b) trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un titolare del trattamento o responsabile del trattamento nell'Unione, ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro;

24) **«obiezione pertinente e motivata»**: un'obiezione al progetto di decisione sul fatto che vi sia o meno una violazione del presente regolamento, oppure che l'azione prevista in relazione al titolare del trattamento o responsabile del trattamento sia conforme al presente regolamento, la quale obiezione dimostra chiaramente la rilevanza dei rischi posti dal progetto di decisione riguardo ai diritti e alle libertà fondamentali degli interessati e, ove applicabile, alla libera circolazione dei dati personali all'interno dell'Unione;

25) **«servizio della società dell'informazione»**: il servizio definito all'articolo 1, paragrafo 1, lettera b), della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio ([19]);

26) **«organizzazione internazionale»**: un'organizzazione e gli organismi di diritto internazionale pubblico a essa subordinati o qualsiasi altro organismo istituito da o sulla base di un accordo tra due o più Stati.

Art.2 - Motivazione e obiettivo del presente Regolamento

Il riutilizzo o lo smaltimento di apparecchiature elettroniche (es. Personal Computer, Server, palmari, tablet-PC etc.) e di supporti di memorizzazione (es. hard disk interni, hard disk esterni, cd-rom, dvd, chiavette usb, schede SD etc.) sono attività estremamente critiche dal punto di vista della sicurezza e della privacy dei dati personali, che devono pertanto essere rigidamente disciplinate.
Accade talvolta infatti che i dati del precedente utilizzatore – in alcuni casi estremamente riservati e delicati - non siano adeguatamente cancellati, e vengano pertanto portati a conoscenza di soggetti terzi non autorizzati; tra i casi più eclatanti che si sono verificati in tempi recenti possiamo evidenziare:

- il rinvenimento da parte dell'acquirente di un disco rigido usato, commercializzato attraverso un sito Internet, di dati bancari relativi a oltre un milione di individui contenuti nel disco medesimo;
- il rinvenimento da parte dell'acquirente di un personal computer usato di decine di files e cartelle relativi alle patologie dei pazienti di una struttura sanitaria pubblica.

Obiettivo del presente regolamento è pertanto assicurare che il riutilizzo o lo smaltimento di apparecchiature elettroniche e di supporti di memorizzazione avvengano in condizioni di sicurezza, con la ragionevole certezza che i dati (personali, sensibili, giudiziari, di qualsiasi tipo) precedentemente memorizzati siano completamente cancellati con modalità tecniche che ne rendano impossibile il recupero.
E' infatti noto che la semplice operazione di cancellazione di in file o di una cartella, seguita dallo "svuotamento del cestino" (in ambiente Windows) non comporta la cancellazione fisica dei dati dal supporto di memorizzazione, che possono quindi essere recuperati con una certa semplicità.
E' pertanto necessario l'utilizzo di programmi di tipo "file wiping" o "file shredding", che comportano la riscrittura dei dati cancellati da sette a trentacinque volte, oppure l'utilizzo di apparati che comportino la smagnetizzazione ("degaussing") dei supporti di memorizzazione.

Art.3 - Ambito di validità e di applicazione del presente Regolamento

Le prescrizioni del presente regolamento si applicano alle seguenti apparecchiature dell'Istituto:

- apparati di tipo "personal computer" fissi o portatili;
- apparati di tipo tablet PC:
- apparati di tipo server;
- supporti di memorizzazione di massa, come ad esempio hard disk interni, hard disk esterni, cd-rom, dvd, chiavette usb, schede SD e più in generale a qualsiasi apparato o dispositivo che possa contenere al suo interno qualsiasi tipo di dato (generico, personale, sensibile, giudiziario etc.).

Art.4 – Responsabilità penale e civile

Dall'inosservanza delle disposizioni contenute nel presente regolamento possono derivare responsabilità di tipo:

- amministrativo pecuniario, fino a 20.000.000,00 Euro, ai sensi dell'art. 83 del GDPR, ed eventualmente

- civile, in caso di danni cagionati a terzi, ai sensi dell'art. 82 del GDPR e dell'art.2050 del Codice Civile.

Art. 5 – Modalità tecniche per la gestione del riutilizzo

In caso di riutilizzo di apparecchiature elettroniche o di supporti di memorizzazione, si dovranno utilizzare appositi programmi di "file wiping" o di "file shredding" che forniscano idonee garanzie di non recuperabilità dei dati cancellati, nemmeno con le apparecchiature più sofisticate.

Sul mercato esistono varie soluzioni software, alcune delle quali di pubblico dominio. Allo stato attuale della tecnologia i programmi di file wiping più affidabili sono i seguenti:

- ***Sdelete***, scaricabile dal sito www.microsoft .com, che è l'utility suggerita dalla Microsoft per tutti i sistemi Windows. Tale utility è conforme ai requisiti dello standard del DOD – Department Of Defense 5220.22-M, e fornisce idonee garanzie che I dati saranno cancellati in modo da renderne tecnicamente impossibile il recupero;
- ***Ashampoo File Wiper***, scaricabile dal sito internet www.ashampoo.it, una tra le utility più diffuse ed affidabili allo stato attuale della tecnologia.

Art.6 – Modalità tecniche per la gestione dello smaltimento

Per lo smaltimento degli apparati e dei supporti di memorizzazione, si dovrà distinguere tra il caso in cui il dispositivo sia ancora funzionante, dai casi in cui il dispositivo non sia funzionante.
Nel primo caso si potranno applicare le modalità tecniche previste per il riutilizzo; nel secondo caso, e cioè nel caso in cui il dispositivo non sia funzionante si dovranno adottare le seguenti tecniche:

- ***Demagnetizzazione****:* la demagnetizzazione ("degaussing") permette l'"azzeramento" delle aree magnetiche delle superfici dei dischi o di altre memorie a stato solido, agendo anche sui circuiti che fanno parte del dispositivo e causandone l'inutilizzabilità successiva.
- ***Distruzione fisica***: in determinati casi è necessario ricorrere alla distruzione fisica dei dispositivi di memoria. Tale procedura è l'unica praticabile con i supporti ottici a sola lettura (CD-ROM, DVD-R), che possono essere distrutti o polverizzati con apposite macchine analoghe ai "tritacarta" in uso negli uffici. Gli hard-disk possono essere resi inutilizzabili aprendone l'involucro protettivo e danneggiando meccanicamente le superfici magnetiche (piatti) con l'azione deformante di uno strumento o con appositi punzonatori.

Art.7 – Autorizzazione preliminare alla cancellazione dei dati

Poiché i dati (personali, sensibili, giudiziari etc.) contenuti negli apparati e nei supporti di memorizzazione costituiscono un prezioso patrimonio dell'Istituto, e tenuto conto del fatto che in alcuni casi vi possono essere obblighi specifici di conservazione dei dati per un periodo minimo, prima di procedere alla cancellazione dei dati, chiunque sia il soggetto che materialmente effettua la cancellazione, dovrà chiedere ed ottenere in forma scritta l'autorizzazione alla cancellazione dei dati.
Detta autorizzazione dovrà essere rilasciata in forma scritta dal Dirigente Scolastico o dal DSGA. Se del caso, detta autorizzazione potrà contenere indicazioni sui dati che prima di essere cancellati devono essere oggetto di salvataggio.

Art.8 – Verbale di corretta esecuzione della cancellazione dei dati

Alla fine delle attività di cancellazione, il soggetto che ha materialmente effettuato le operazioni dovrà compilare apposito verbale nel quale dichiara di aver personalmente effettuato la cancellazione in forma permanente dei dati e il buon esito delle operazioni effettuate.

Il suddetto verbale dovrà inoltre contenere i riferimenti (es. marca, modello, numero di serie etc.) dell'apparato o del supporto oggetto del trattamento.

Art.9 – Soggetti tenuti alla verifica del presente regolamento

La responsabilità di vigilare sulla corretta applicazione del presente Regolamento è affidata al DPO – Data Protection Officer (Responsabile della protezione dei dati personali) dell'Istituto, che per il Liceo "G.Galilei" è il Dott. Giancarlo Favero della Ditta Capital Security Srls (www.capitalsecurity.it), con sede in Via Montenapoleone 8 – 20121 Milano (email: giancarlo.favero@capitalsecurity.it – tel. 335-5950674).