6.3 VALUTAZIONE DEL RISCHIO - IC di Monterenzio BO - SEDE Amministrazione
- DATI DEI DIPENDENTI -

PERSONALE COINVOLTO: Vedi lettere di Incarico per Autorizzati e Responsabili del trattamento

Base Giuridica, Termine Cancellazione Dati, Comunicazione a terzi, Categorie di Destinatari e Trasferimento dei Dati
Vedi File c.d. "Registro delle Attività di Trattamento"

LEGENDA (Vedi P. 6.1 del Sistema di gestione): **P.**: Probabilità (da 1 a 4); **D.**: Danno/Gravità (da 1 a 4); **R**: Rischio (da 1 a 16)

Categoria dati personali	P*D	R	Livello Rischio
DATI di DIPENDENTE ORDINARIO	3X1	3	*Modesto*
DATI di DIPENDENTE ai sensi degli artt. 9 e 10 (ES. DISAGIO, PATOLOGIE, SINDACATI, RELIGIONE, DATI GIUDIZIARI, ECC)	2X4	8	*Rilevante*

DESCRIZIONE DEL RISCHIO: Processo di Trattamento

I dati dei DIPENDENTI **ordinari** sono dati comuni riconducibili all'anagrafica e ai dati utilizzati all'interno del rapporto contrattuale con impatto/conseguenza sulla libertà dell'interessato modesta. Le misure adottate appaiono sufficienti.
I dati dei DIPENDENTI con **certificazioni,** pur essendo trattati unicamente all'interno del rapporto contrattuale lavorativo richiedono invece una valutazione del rischio residuo.

MISURE DI SICUREZZA ADOTTATE

Dati digitali/informatici= 1. L'Organizzazione si è appoggiata alle softwarehouse NUVOLA, MEDIASOFT, GOOGLE FOR EDU e SIDI. L'Istituto sta implementando le misure di sicurezza obbligatorie del Regolamento UE (art. 32 e ss.), e le misure minime Agid - ICT (Es. credenziali d'accesso controllate; politica di Backup; presenza di un Firewall; cablaggio della rete con sottoreti univoche; Gruppo di continuità presente; Politica password; ecc.). 2. Le nomine ad incaricati sono state trascritte. 3. i dati conservati sui PC interni all'Istituto sono protetti da accesso controllato, limitato ai compiti della funzione di riferimento. 4. l'Istituto si è dotato di una politica scritta di backup. 5. l'accesso all'Istituto è controllato. 6. Il sistema informativo dell'ente risponde alle indicazioni fornite da AGiD per le misure minime di sicurezza ICT. I dati memorizzati su supporto informatico sono gestiti all'interno di tale sistema. I dati riportati su documentazione e registri cartacei seguono le procedure indicate nel manuale di gestione del protocollo cartaceo. Se il trattamento è svolto in parte o nella sua interezza da un responsabile esterno, l'Istituto delega tale organizzazione tramite un atto specifico alla sicurezza e alla protezione dei dati.

Dati cartacei= L'Organizzazione conserva i "dati particolari" dei **Dipendenti** in armadi chiusi a chiave nella Segreteria organizzativa, in particolare sotto chiave o in busta chiusa. Per consultare il proprio fascicolo, l'interessato compila l'apposita richiesta d'accesso, convalidata dal Titolare del Trattamento; l'atto della consultazione avviene sotto supervisione. La sede amministrativa dell'Istituto è protetta da allarme.

VALUTAZIONE ADEGUATEZZA DELLE MISURE DI SICUREZZA ADOTTATE: Vedi allegato "Analisi Misure di Sicurezza"

PROGRAMMA DELLE MISURE DI PREVENZIONE E PROTEZIONE

Intervento da attuare	Responsabilità	Scadenza
Informazione e formazione	Titolare	Secondo il piano definito nel sistema GDPR in M 7.2.1 Piano Formazione
Impletazione della linee guida contenute nelle Politica Operative:i Password, clear desk clear screen, utilizzo accettabile, access control, gestioni degli incidenti.	Titolare	In sede di Riesame della direzione
Verifica delle condizioni operative e dei requisiti tecnici di sicurezza	Titolare	Cadenza semestrale da parte di Responsabile IT e RSG/DPO ove presente

FINALITA' DI TRATTAMENTO e FREQUENZA DI TRATTAMENTO

Adempimento degli obblighi istituzionali I Giornaliera

RISCHIO RESIDUO

Date le misure di sicurezza adottate e pianificate si considera il rischio residuo dell'attività di trattamento **accettabile**.

DATA	FIRMA TITOLARE TRATTAMENTO
02/09/2024	
DATA	**FIRMA DPO**
02/09/2024	

6.3 VALUTAZIONE DEL RISCHIO - IC di Monterenzio BO - SEDE Amministrazione
- DATI DEI FORNITORI -

PERSONALE COINVOLTO: Vedi lettere di Incarico per Autorizzati e Responsabili del trattamento

Base Giuridica, Termine Cancellazione Dati, Comunicazione a terzi, Categorie di Destinatari e Trasferimento dei Dati
Vedi File c.d. "Registro delle Attività di Trattamento"

LEGENDA (Vedi P. 6.1 del Sistema di gestione): **P.**: Probabilità (da 1 a 4); **D.**: Danno/Gravità (da 1 a 4); **R**: Rischio (da 1 a 16)

Categoria dati personali	P*D	R	Livello Rischio
DATI ANAGRAFICI	2X1	2	*Modesto*
DATI PARTICOLARI (AUTODICHIARAZIONE ai sensi dell'art. 10 GDPR 679/16 e dell'art. 46, 47 e 76 e ss. del D.p.r. 445/2000, TRACCIABILITA' DEI FLUSSI, ECC...)	2X4	8	*Rilevante*

DESCRIZIONE DEL RISCHIO: Processo di Trattamento

I dati dei FORNITORI ordinari sono dati **comuni** riconducibili all'anagrafica e ai dati utilizzati all'interno del rapporto contrattuale con impatto/conseguenza sulla libertà dell'interessato modesta. Le misure adottate appaiono sufficienti.
I Dati dei FORNITORI riconducibili a dati **particolari**, pur essendo trattati unicamente all'interno del rapporto contrattuale lavorativo richiedono invece una valutazione del rischio residuo.

MISURE DI SICUREZZA ADOTTATE

Dati digitali/informatici= 1. L'Organizzazione si è appoggiata alle softwarehouse NUVOLA, MEDIASOFT, GOOGLE FOR EDU e SIDI. L'Istituto sta implementando le misure di sicurezza obbligatorie del Regolamento UE (art. 32 e ss.), e le misure minime Agid - ICT (Es. credenziali d'accesso controllate; politica di Backup; presenza di un Firewall; cablaggio della rete con sottoreti univoche; Gruppo di continuità presente; Politica password; ecc.). 2. Le nomine ad incaricati sono state trascritte. 3. i dati conservati sui PC interni all'Istituto sono protetti da accesso controllato, limitato ai compiti della funzione di riferimento. 4. l'Istituto si è dotato di una politica scritta di backup. 5. l'accesso all'Istituto è controllato. 6. Il sistema informativo dell'ente risponde alle indicazioni fornite da AGiD per le misure minime di sicurezza ICT. I dati memorizzati su supporto informatico sono gestiti all'interno di tale sistema. I dati riportati su documentazione e registri cartacei seguono le procedure indicate nel manuale di gestione del protocollo cartaceo. Se il trattamento è svolto in parte o nella sua interezza da un responsabile esterno, l'Istituto delega tale organizzazione tramite un atto specifico alla sicurezza e alla protezione dei dati.

Dati cartacei= L'Organizzazione conserva i "dati particolari" dei **Fornitori** in armadi chiusi a chiave nella Segreteria organizzativa, in particolare sotto chiave o in busta chiusa. Per consultare il proprio fascicolo, l'interessato compila l'apposita richiesta d'accesso, convalidata dal Titolare del Trattamento; l'atto della consultazione avviene sotto supervisione. La sede amministrativa dell'Istituto è protetta da allarme.

VALUTAZIONE ADEGUATEZZA DELLE MISURE DI SICUREZZA ADOTTATE: Vedi allegato "Analisi Misure di Sicurezza"

PROGRAMMA DELLE MISURE DI PREVENZIONE E PROTEZIONE

Intervento da attuare	Responsabilità	Scadenza
Informazione e formazione	Titolare	Secondo il piano definito nel sistema GDPR
Verifica delle condizioni operative e dei requisiti tecnici di sicurezza	Titolare	Cadenza semestrale da parte di Responsabile IT e RSG/DPO ove presente

FINALITA' DI TRATTAMENTO e FREQUENZA DI TRATTAMENTO

Adempimento degli obblighi istituzionali I Giornaliera

RISCHIO RESIDUO

Date le misure di sicurezza adottate e pianificate si considera il rischio residuo dell'attività di trattamento **accettabile**.

DATA	FIRMA TITOLARE TRATTAMENTO
02/09/2024	
DATA	**FIRMA DPO**
02/09/2024	

6.3 VALUTAZIONE DEL RISCHIO - IC di Monterenzio BO - Sede Amministrazione
- DATI DEGLI ALUNNI -

PERSONALE COINVOLTO: Vedi lettere di Incarico per Autorizzati e Responsabili del trattamento

Base Giuridica, Termine Cancellazione Dati, Comunicazione a terzi, Categorie di Destinatari e Trasferimento dei Dati
Vedi File c.d. "Registro delle Attività di Trattamento"

LEGENDA (Vedi P. 6.1 del Sistema di gestione): **P.**: Probabilità (da 1 a 4); **D.**: Danno/Gravità (da 1 a 4); **R**: Rischio (da 1 a 16)

Categoria dati personali	P*D	R	Livello Rischio
ALUNNO ORDINARIO *Tipo di Dati personali trattati: dati anagrafici, stato civile, soggetti a carico, ISEE, ecc.*	3X1	3	*Modesto*
ALUNNI CON CERTIFICAZIONI *Tipo di Dati personali trattati: Dati sanitari (es. BES, PEI, DVA, DSA, PDP, DISAGI, PATOLOGIE ECC)*	2X4	8	*Rilevante*

DESCRIZIONE DEL RISCHIO: Processo di Trattamento

I dati degli ALUNNI ordinari sono dati **comuni** riconducibili all'anagrafica e ai dati utilizzati all'interno del rapporto contrattuale con impatto/conseguenza sulla libertà dell'interessato modesta. Le misure adottate appaiono sufficienti.
I dati degli ALUNNI con **certificazioni**, pur essendo trattati unicamente all'interno del rapporto D'ISCRIZIONE richiedono invece una valutazione del rischio residuo.

MISURE DI SICUREZZA ADOTTATE

Dati digitali/informatici= 1. L'Organizzazione si è appoggiata alle softwarehouse NUVOLA, MEDIASOFT, GOOGLE FOR EDU e SIDI. L'Istituto sta implementando le misure di sicurezza obbligatorie del Regolamento UE (art. 32 e ss.), e le misure minime Agid - ICT (Es. credenziali d'accesso controllate; politica di Backup; presenza di un Firewall; cablaggio della rete con sottoreti univoche; Gruppo di continuità presente; Politica password; ecc.). 2. Le nomine ad incaricati sono state trascritte. 3. i dati conservati sui PC interni all'Istituto sono protetti da accesso controllato, limitato ai compiti della funzione di riferimento. 4. l'Istituto si è dotato di una politica scritta di backup. 5. l'accesso all'Istituto è controllato. 6. Il sistema informativo dell'ente risponde alle indicazioni fornite da AGiD per le misure minime di sicurezza ICT. I dati memorizzati su supporto informatico sono gestiti all'interno di tale sistema. I dati riportati su documentazione e registri cartacei seguono le procedure indicate nel manuale di gestione del protocollo cartaceo. Se il trattamento è svolto in parte o nella sua interezza da un responsabile esterno, l'Istituto delega tale organizzazione tramite un atto specifico alla sicurezza e alla protezione dei dati.

Dati cartacei= L'Organizzazione conserva i "dati particolari" degli **Alunni** in armadi chiusi a chiave nella Segreteria organizzativa, in particolare sotto chiave o in busta chiusa. Per consultare il proprio fascicolo, l'interessato compila l'apposita richiesta d'accesso, convalidata dal Titolare del Trattamento; l'atto della consultazione avviene sotto supervisione. La sede amministrativa dell'Istituto è protetta da allarme.

VALUTAZIONE ADEGUATEZZA DELLE MISURE DI SICUREZZA ADOTTATE: Vedi allegato "Analisi Misure di Sicurezza"

PROGRAMMA DELLE MISURE DI PREVENZIONE E PROTEZIONE

Intervento da attuare	Responsabilità	Scadenza
Informazione e formazione	Titolare	Secondo il piano definito nel sistema GDPR
Verifica delle condizioni operative e dei requisiti tecnici di sicurezza	Titolare	Cadenza semestrale da parte di Responsabile IT e RSG/DPO ove presente

FINALITA' DI TRATTAMENTO e FREQUENZA DI TRATTAMENTO

Adempimento degli obblighi istituzionali I Giornaliera

RISCHIO RESIDUO

Date le misure di sicurezza adottate e pianificate si considera il rischio residuo dell'attività di trattamento **accettabile**.

DATA	FIRMA TITOLARE TRATTAMENTO
02/09/2024	
DATA	**FIRMA DPO**
02/09/2024	

6.3 VALUTAZIONE DEL RISCHIO PRIVACY ART. 35 DEL GDPR - IC di Monterenzio BO - Alunni & Famiglie, Dipendenti e Fornitori

CLASSE RISCHIO	RISCHIO di dettaglio (possono essere ripetuti per più categorie)	FATTORI	Probabilità	Impatto/Gravità	RISCHIO residuo
RID	utilizzo/accesso di/da dispositivi non inventariati (Pc, Tablet, Smartphone,...) anche in lavoro agile	US	2	3	6
RD	predisposizione e attivazione di software/hardware/reti per il controllo degli accessi da remoto (Teamviewer e/o VPN)	US	2	3	6
RID	perdita e/o divulgazione di dato sanitario a seguito dell'obbligo di autodichiarazione dei dipendenti (vedi allegato)	US	1	3	3
RD	replica dei dati su supporto non sicuro/adatto	U	3	3	9
R	installazione di software non autorizzato sulla postazione di lavoro	U	1	3	3
R	divulgazione involontaria delle informazioni (es in un dialogo)	U	2	2	4
R	attacco di ingegneria sociale per carpire informazioni/furto identità	U	2	4	8
R	mancata protezione dei pc (es. schermi non protetti)	U	2	3	6
R	cambio mansione, dimissioni di dipendente	U	2	2	4
R	affidamento di attività di progetto/servizio a fornitori	U	3	2	6
RID	gestione/conservazione dei dati tramite fornitori scelti a supporto della didattica	US	3	3	9
RID	infezioni da virus/malware	S	3	3	9
R	sistema di autenticazione/profilazione/gestione delle credenziali non adeguato	S	3	3	9
RID	errori/vulnerabilità nel software utilizzato	S	2	2	4
R	trasmissioni di dati in maniera non sicura	S	3	3	9
I	installazione di un middleware, software o hw che danneggia i dati	S	1	4	4
RI	comportamenti sleali o fraudolenti di dipendenti	U	2	4	8
ID	errori in fase di aggiornamento dei SO, del middleware, delle configurazioni	US	1	3	3
ID	errori umani involontari di dipendenti (es per poca formazione/competenza, disattenzione, ..)	U	2	4	8
D	evento naturale catastrofico (incendio, inondazione)	C	1	4	4
D	evento vandalico	C	2	2	4
RD	furto di dispositivi (pc, telefono, ipad, hw)	C	2	3	6
D	utilizzo di sw contraffatto/senza licenza	U	1	3	3
D	dimensionamento non corretto dei repository dei dati (DB, file system)	U	1	2	2
D	errori in fase di aggiornamento dei sw applicativo	U	1	3	3
D	scadenza licenza, mancato aggiornamento software	U	1	2	2
D	interruzioni o non disponibilità della rete (guasti)	C	1	3	3
D	indisponibilità del personale (malattia, sciopero, pensionamento, ..)	U	1	2	2
D	furto documenti cartacei	C	2	4	8
D	guasto hardware	S	1	4	4
D	attacchi DOS/DDOS (Distributed Denial of Service)	S	2	4	8
D	interruzioni o non disponibilità dei sistemi complementari (elettricità, climatizzazione, ecc.)	C	1	2	2
RD	archiviazione eseguita in modo incorretto - documenti cartacei NON sensibili	C	2	2	4

R	Riservatezza	U	Comportamento umano
I	Integrità	S	Eventi relativi agli strumenti
D	Disponibilità	C	Eventi relativi al contesto

6.3 TABELLE DI SUPPORTO PER LA VALUTAZIONE - IC di Monterenzio BO

PRIVACY CONTROL

Valutazione dell'Impatto/Gravità

Impatto	Livello	descrizione
4	Grave	Individui che possono avere conseguenze significative, o addirittura irreversibili, che non possono superare (incapacità di lavorare, disturbi psicologici o fisici a lungo termine, morte, ecc.).
3	Significativo	Gli individui possono incontrare conseguenze significative, che dovrebbero essere in grado di superare anche se con gravi difficoltà (perdita significativa di denaro, inserimento di liste nere da parte di istituti finanziari, danni alla proprietà, perdita di posti di lavoro, citazione in giudizio, peggioramento della salute, ecc.).
2	Moderato	Gli interessati possono incontrare significativi disagi, che saranno in grado di superare nonostante alcune difficoltà (costi aggiuntivi, rifiuto di accesso ai servizi, paura, mancanza di comprensione, stress, disturbi fisici minori, ecc.).
1	Trascurabile	Gli interessati non incontrano inconvenienti significativi

Valutazione della probabilità

Probabilità	Liv.	Criterio probabilistico (prob. di accadimento stimata nell'anno)
4	Quasi certo	Prob.>50%
3	Probabile	20%<Prob.<50%
2	Moderata	5%<Prob.<20%
1	Rara	Prob.<5%

	IMPROBABILE= 1	POSSIBILE (POCO PROB.)= 2	PROBABILE = 3	ALTAMENTE PROBABILE = 4
GRAVI = 4	4	8	12	16
SIGNIFICATIVI = 3	3	6	9	12
MODESTA ENTITÀ = 2	2	4	6	8
LIEVI = 1	1	2	3	4

6.4 ANALISI PRELIMINARE e VALUTAZIONE DI IMPATTO SOFTWAREHOUSE & PIAT MULT - IC di Monterenzio BO -

PRIVACY CONTROL

Tipologia	Fornitore	Indirizzo/sede	ELEMENTI/CARATTERISTICHE ANALIZZATI																		check (somma dei pesi relativi = 100)
			Livello di conoscenza e di gradimento c/o famiglie alunni		Peso relativo (importanza) dell'elemento	Livello di conoscenza c/o docenti		Peso relativo (importanza) dell'elemento	Livello di efficacia/ efficienza piattaforma (metodologia didattica)		Peso relativo (importanza) dell'elemento	Livello di efficacia/ efficienza piattaforma (caratteristiche tecniche)		Peso relativo (importanza) dell'elemento	Livello delle modalità di gestione della piattaforma		Peso relativo (importanza) dell'elemento	Livello di sicurezza informatica e protezione privacy della piattaforma		Peso relativo (importanza) dell'elemento	
					10			10			17			17			13			33	100
			Valore dell'elemento		Valore relativo	Valore dell'elemento		Valore relativo	Valore dell'elemento		Valore relativo	Valore dell'elemento		Valore relativo	Valore dell'elemento		Valore relativo	Valore dell'elemento		Valore relativo	Valore percentuale finale
REGISTRO ELETTRONICO/ SEGRETERIA DIGITALE	NUVOLA	ITALIA	Alto		20	Alto	x	30	Alto	x	51	Alto		34	Alto	x	39	Alto	x	99	91%
			Medio	x		Medio			Medio			Medio	x		Medio			Medio			
			Basso			Basso			Basso			Basso			Basso			Basso			
PIATTAFORMA MULTIMEDIALE	GOOGLE WORKSPACE	CALIFORNIA	Alto		10	Alto		10	Alto	x	51	Alto		51	Alto	x	13	Alta	x	99	78,00%
			Medio			Medio			Medio			Medio	x		Medio			Medio			
			Basso	x		Basso	x		Basso			Basso			Basso			Basso			

LEGENDA	ROSSO (Vpf < 60%) Sconsigliato. Da utilizzare solo in casi particolari e con autorizzazione del DS	GIALLO (60% ≤ Vpf ≤ 75%) Da utilizzare per prestazioni specifiche (ad es., video lezioni)	VERDE (Vpf >75%) Consigliato

Conclusioni: le piattaforme sottoposte ad analisi sono state scelte sulla base delle indicazioni presenti sul sito del Ministero dell'Istruzione e delle conoscenze esistenti all'interno dell'Istituto. Sulla base delle valutazioni effettuate tenendo conto del parere dello staff dirigenziale, dello staff degli animatori digitali e del Consiglio d'Istituto, si decide di adottare per la didattica: il registro elettronico "NUVOLA" con tutte le sue applicazioni interne (assegno compiti, restituzione compiti, segnalazioni link, agenda, scambio di file, videoconferenza integrata ecc), ed in alternativa gli applicativi di GOOGLE WORKSPACE. Per le videolezioni si possono utilizzare entrambi i portali effettuando i collegamenti sia dal registro elettronico che dell'apposita area delle videolezioni.

IL DIRIGENTE SCOLASTICO

Firma autografa sostituita a mezzo stampa ai sensi dell'art. 3 comma 2 D.L.vo n.39/1993

TABELLA DI SUPPORTO PER LA VALUTAZIONE

Valutazione criterio	CRITERI					
	Livello di conoscenza e di gradimento c/o famiglie alunni	**Livello di conoscenza c/o docenti**	**Livello di efficacia/ efficienza piattaforma (metodologia didattica)**	**Livello di efficacia/ efficienza piattaforma (caratteristiche tecniche)**	**Livello delle modalità di gestione della piattaforma**	**Livello di sicurezza informatica e protezione privacy della piattaforma**
ALTO	La piattaforma è molto conosciuta e utilizzata	La piattaforma è molto conosciuta e utilizzata	La piattaforma consente un elevato apporto di didattica attiva (flipped classroom, project work, inclusione per soggetti con disabilità, ecc.)	La piattaforma ha caratteristiche tecniche notevoli (affidabilità, qualità della prestazione, scarse possibilità d'interruzioni o di malfunzionamenti, ecc.)	La piattaforma è facile da gestire e non richiede particolari risorse (non richiede un amministratore di sistema, non richiede che sia nominata responsabile del trattamento)	La piattaforma garantisce un elevato standard di sicurezza e di privacy
MEDIO	La piattaforma è sufficientemente conosciuta e utilizzata solo per necessità	La piattaforma è sufficientemente conosciuta e utilizzata per necessità e/o nelle sue funzioni essenziali	La piattaforma consente un esercizio sufficiente di didattica attiva	La piattaforma ha caratteristiche tecniche sufficienti con qualche piccolo disagio	La piattaforma consente una gestione con un minimo d'impiego di particolari risorse (richiede che sia nominato come responsabile del trattamento e richiede un amministratore di sistema)	La piattaforma garantisce uno standard di sicurezza e di privacy sufficiente
BASSO	La piattaforma non è conosciuta e potrebbe essere utilizzata con qualche o notevole difficoltà	La piattaforma non è conosciuta, potrebbe essere utilizzata con qualche o notevole difficoltà e ha bisogno di formazione	La piattaforma consente un esercizio modesto o nullo di didattica attiva	La piattaforma ha caratteristiche tecniche insufficienti con disagi importanti	La piattaforma richiede una gestione complicata (ad es., sono necessari accounting specifici, richiede un amministratore di sistema, è difficile o praticamente impossibile nominarla amministratore di sistema)	La piattaforma garantisce uno standard di sicurezza e di privacy basso

IC di Monterenzio BO - DESCRIZIONE DETTAGLIATA DELLE MISURE DI SICUREZZA ai sensi del GDPR n. 679/16 - 6.3

Il foglio riporta un ELENCO NON ESUSTIVO DELLE MISURE che possono essere adottate per ridurre i rischi. E' necessario valutare di volta in volta quali misure sono utilizzabili a riduzione dei singoli rischi.
Le misure sono tratte da CNIL - tool di valutazione d'impatto sulla privacy - VEDI ALLEGATO MISURE DI SICUREZZA ai sensi dell'Art. 32 e ss del GDPR 679/16

tipologia di misura	misura	descrizione/esempi
controlli di sicurezza funzionali	crittografia	mezzi implementati per assicurare la confidenzialità dei dati archiviati (in database, file, backup etc.), così come le procedure per gestire chiavi crittografiche (creazione, archiviazione, aggiornamento in caso di compromissione etc.)
controlli di sicurezza funzionali	anonimizzazione	
controlli di sicurezza funzionali	partizionamento dei dati	
controlli di sicurezza funzionali	controllo degli accessi	
controlli di sicurezza funzionali	tracciabilità	es gestione dei log
controlli di sicurezza funzionali	archiviazione	processi di gestione dell'archivio (consegna, archiviazione, consultazione etc.). Specificare i ruoli relativi all'archivio (ufficio di origine, agenzie di trasferimento etc.) e la politica di archiviazione.
controlli di sicurezza funzionali	sicurezza dei documenti cartacei	sono definite le regole per la conservazione dei documenti cartacei contenenti dati utilizzati durante il trattamento, come sono stampati, archiviati, distrutti e scambiati.
controlli di sicurezza funzionali	minimizzazione della quantità dei dati personali	rientrano misure di filtraggio e rimozione, riduzione della sensibilità attraverso la conversione, ridurre la natura identificativa del dato, ridurre l'accumulazione dei dati, limitare l'accesso ai dati
controlli di sicurezza funzionali	utilizzo di strumenti e servizi per la didattica	sono definite le regole di accesso e di utilizzo dei contenuti e servizi didattici per la gestione della didattica.
controlli di sicurezza fisici	minimizzazione della vulnerabilità delle risorse utilizzate nel trattamento	(es politiche di aggiornamento del software, test del software utilizzato, limitazioni dell'accesso fisico al materiale che contiene dati personali)
controlli di sicurezza fisici	controlli per infezioni da malware e virus	(misure per proteggere l'accesso di infezioni a reti, postazioni, server)
controlli di sicurezza fisici	gestione delle postazioni di lavoro	Misure adottate per ridurre la possibilità che le caratteristiche del software (sistemi operativi, applicazioni aziendali, software per ufficio, impostazioni etc.) vengano sfruttate per danneggiare i dati personali (aggiornamenti, protezione fisica e accesso, lavoro su uno spazio di rete di backup, controlli di integrità logging etc.).
controlli di sicurezza fisici	backup	Politiche e mezzi implementati per assicurare la disponibilità o l'integrità dei dati personali, mentre si mantiene la loro confidenzialità
controlli di sicurezza fisici	manutenzione delle infrastrutture	politica di manutenzione fisica degli apparati IT e dei sistemi complementari
controlli di sicurezza fisici	contratti di trattamento	Regolare i rapporti di approvvigionamento (es. responsabile trattamento dati, responsabile protezione dei dati, servizi cloud, ecc) tramite un contratto che riporti ad esempio: - Richiedere al fornitore di inoltrare la sua politica di sicurezza dei sistemi informativi insieme a tutti i documenti di supporto delle sue certificazioni di sicurezza delle informazioni e allegare tali documenti al contratto. Garantire che le misure siano conformi alla propria politica di sicurezza ed alle raccomandazioni dell'autorità garante. - Determinare e fissare in modo preciso, su base contrattuale, le operazioni che il responsabile del trattamento potrà eseguire sui dati personali: 1) I dati a cui avrà accesso o che gli saranno trasmessi. 2) Le operazioni che deve eseguire sui dati. 3) La durata per la quale può memorizzare i dati. 4) Tutti i destinatari a cui il responsabile del trattamento potrà trasmettere i dati. 5) Le operazioni da eseguire al termine del servizio (cancellazione permanente dei dati o restituzione dei dati nel contesto della reversibilità quindi distruzione di dati). 6) Gli obiettivi di sicurezza stabiliti dal titolare del trattamento. - Determinare, su base contrattuale, la ripartizione delle responsabilità in merito ai processi legali volti a consentire agli interessati di esercitare i propri diritti. Esplicitamente vietare o regolare l'utilizzo di fornitori di secondo livello. - Chiarire nel contratto che il rispetto degli obblighi di protezione dei dati è un requisito vincolante del contratto.
controlli di sicurezza fisici	monitoraggio delle attività di rete (incidenti di sicurezza)	Esistenza di misure messe in atto per essere in grado di rilevare tempestivamente incidenti relativi a dati personali e di disporre elementi utilizzabili per studiarli o fornire elementi di prova nel contesto delle indagini (politica di registrazione eventi, rispetto degli obblighi di protezione dei dati etc.)
controlli di sicurezza fisici	controlli degli accessi fisici	Politiche per assicurare la sicurezza fisica (zonizzazione, accompagnamento, uso di tornelli, porte chiuse e così via). Procedure di avviso in caso di irruzione.
controlli di sicurezza fisici	sicurezza dell'hardware	Esistenza delle misure adottate per ridurre la possibilità che le caratteristiche delle apparecchiature (server, postazioni fisse, portatili, periferiche, dispositivi di comunicazione, supporti rimovibili etc.) vengano utilizzate per danneggiare i dati personali (inventario, compartimentalizzazione, ridondanza, limiti per l'accesso etc.)
controlli di sicurezza fisici	Evitare le fonti di rischio	Esistenza di misure per prevenire le fonti di rischio, umane o non umane, che possono essere incontrate a scapito dei dati personali (merci pericolose, aree geografiche pericolose, trasferimento dati al di fuori dell'UE etc.)
controlli di sicurezza fisici	Protezione contro fonti di rischio non umane	Esistenza di misure per ridurre o evitare i rischi connessi a fonti non umane (fenomeni climatici, incendio, danni provocati dall'acqua, incidenti interni o esterni, animali, etc.) che potrebbero influire sulla sicurezza dei dati personali (misure preventive, rilevamento, protezione etc.
controlli d'organizzazione	Organizzazione privacy	Esistenza di un'organizzazione in grado di dirigere e controllare la protezione dei dati personali all'interno dell'organizzazione (designazione di un DPO, creazione di un organo di monitoraggio, etc.)
controlli d'organizzazione	Politiche privacy	Il titolare del trattamento dei dati deve disporre di una banca dati documentale che formalizzi gli obiettivi e le regole da applicare nel campo della protezione dei dati (rischi, principi chiave da seguire, obiettivi, regole da applicare, ecc., revisione periodica della politica IT etc.)
controlli d'organizzazione	Gestione dei rischi sulla privacy	Esistenza di una politica che definisce i processi volti a controllare i rischi che i trattamenti dell'organizzazione pongono sui diritti e le libertà delle persone interessate (censimento del trattamento dei dati personali, quali dati sono, valutazione del rischio, determinare misure esistenti o previste etc.)
controlli d'organizzazione	Integrare la protezione della privacy nei progetti	Esistenza di procedure che descrivono i metodi per tenere conto della protezione dei dati personali in qualsiasi nuovo trattamento (etichette di fiducia, norme, gestione del rischio per la persona interessata secondo una metodologia etc.)
controlli d'organizzazione	Gestire le violazioni dei dati personali	Esistenza di un'organizzazione oeprativa per rilevare e gestire eventi che possono influire sulle libertà e sulla privacy delle persone interessate (definizione delle responsabilità a piano di reazione, caratterizzazione delle violazioni etc.)
controlli d'organizzazione	Gestione del personale	Esistenza di un piano di formazione in materia di potezione dei dati e procedure/istruzioni che descrivono le istruzioni per l'accesso ai dati .
controlli d'organizzazione	Relazioni con terze parti	Esistenza di una procedura per ridurre i rischi che l'accesso legittimo ai dati da parte di terzi possa porre alle libertà della vita privata delle persone interessate (identificazione dei terzi, contratto di subappalto, convenzione etc.)
controlli d'organizzazione	supervisione	Esistenza di misure per fornire una visione globale e aggiornata dello stato di protezione dei dati e conformità con il GDPR (per monitorare la conformità di trattamenti, obiettivi e indicatori, responsabilità ,etc).