ASP Collegio Morigi
De Cesaris

MANUALE DI CONFORMITA' PRIVACY GDPR

EMISSIONE ANNO 2024

(da riemettersi entro fine anno solare successivo)

Documento di certificazione dei requisiti di conformità,
predisposto in riferimento al **criterio dell'accountability**,
sancito dall'Art.5, comma2 del Reg.UE 2016/679

VALIDAZIONE DEL DOCUMENTO

.....
(Timbro/Firma del Titolare del trattamento
o strumento di validazione elettronica tramite tecnologia ad accesso riservato del Titolare)

© Documento valido ed utilizzabile dal Titolare del trattamento esclusivamente a fini di conformità interna

SOMMARIO

ALLEGATI:
GDPR-2-Data breach
GDPR-2-Diritti interessati
GDPR-3-Nomina autorizzati
GDPR-3-Nomina esterni
GDPR-4-Informative (modelli vari, vedi cap.7)

APPENDICI:
1-Schede trattamenti
2-Policy sicurezza informatica (abstract)

© Documento valido ed utilizzabile dal Titolare del trattamento esclusivamente a fini di conformità interna

1) PRINCIPI GENERALI IN MATERIA DI PROTEZIONE DEI DATI

1.1) Il diritto fondamentale alla protezione dei dati

La protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è un **diritto fondamentale**. L'articolo 8, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea («Carta») e l'articolo 16, paragrafo 1, del trattato sul funzionamento dell'Unione europea («TFUE») stabiliscono che **ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano**. Sulla base di tale principio l'Unione Europea ha ritenuto di emanare uno specifico Regolamento (**GDPR**), contenente i principi e le norme a tutela delle persone fisiche con riguardo al trattamento dei dati personali finalizzato a garantirne i diritti e le libertà fondamentali, in particolare il diritto alla protezione dei dati personali, a prescindere dalla loro nazionalità o dalla loro residenza. Il GDPR è inteso a contribuire alla realizzazione di uno spazio di libertà, sicurezza e giustizia, al progresso economico e sociale, al rafforzamento e alla convergenza delle economie nel mercato interno e al benessere delle persone fisiche

1.2) I principi generali in materia di privacy

La scrivente organizzazione, di seguito identificata "Collegio Morigi", tramite l'implementazione ed attuazione del presente modello, garantisce l'applicazione dei principi fondamentali della privacy, sanciti dal GDPR ed identificati nella seguente tabella.

PRINCIPIO GENERALE E RIFERIMENTO DI LEGGE	DESCRIZIONE
LICEITÀ, CORRETTEZZA E TRASPARENZA (GDPR, Art.5, c.1, l.a)	Ogni trattamento di dati è legittimato da specifici requisiti, quali un consenso espresso dell'interessato, un obbligo di legge, un contratto tra le parti, un interesse legittimo del titolare. I dati sono trattati in modo corretto e trasparente nei confronti dell'interessato
FINALITÀ' (GDPR, Art.5, c.1, l.b)	I dati personali sono raccolti e trattati solo per finalità predeterminate, esplicite e legittime
NECESSITÀ', NON ECCEDENZA, ESSENZIALITÀ (GDPR, Art.5, c.1, l.c)	L'utilizzo dei dati personali è sempre ridotto al minimo necessario essenziale per il raggiungimento delle finalità dichiarate; i dati personali sono raccolti e trattati solo se funzionali al raggiungimento delle finalità dichiarate; i dati personali sono trattati con modalità e strumenti proporzionali alle finalità da raggiungere
ESATTEZZA, COMPLETEZZA, AGGIORNAMENTO (GDPR, Art.5, c.1, l.d)	I dati personali sono puntualmente verificati, in modo che sia garantita la loro esattezza, completezza ed aggiornamento
CONSERVAZIONE (GDPR, Art.5, c.1, l.e)	I dati personali sono conservati per un periodo di tempo limitato al raggiungimento delle finalità dichiarate
SICUREZZA (GDPR, Art.5, c.1, l.f)	i dati sono sempre raccolti e trattati previa adozione di idonee misure di sicurezza
RISERVATEZZA (GDPR, Art.5, c.1, l.f)	i dati sono trattati da soggetti adeguatamente identificati, autorizzati ed istruiti

SCOPO DOCUMENTATIVO: Il presente documento e relativi allegati, riportano adeguate e complete evidenze in merito ai suddetti principi generali, ottemperando al requisito di Accountability previsto dall'Art.5, comma 2 del GDPR ***("il Titolare è competente per il rispetto dei principi generali in materia di privacy ed in grado di comprovarlo")***

SCOPO ORIENTATIVO Il presente documento definisce le linee guida generali da implementare, aggiornare e rispettare per garantire il pieno rispetto dei requisiti normativi in materia di privacy.

© Documento valido ed utilizzabile dal Titolare del trattamento esclusivamente a fini di conformità interna

2) VALIDITÀ, RECEPIMENTO NORMATIVO E CONTESTO

Il presente documento:

- **certifica e documenta il sistema di conformità privacy GDPR di Collegio Morigi;**
- **viene emesso alla data indicata in intestazione, recependo il contesto normativo in vigore (di seguito classificato);**
- **ha validità fino alla sua riemissione, da effettuarsi entro il termine dell'anno solare successivo alla data di emissione.**

Il sistema di conformità privacy è implementato in relazione ai requisiti delle seguenti norme comunitarie e nazionali:

- Regolamento UE 2016/679 "**General Data Protection Regulation**";
- D.Lgs.196/2003 "Codice Privacy", come modificato ed integrato da D.Lgs.101/2018.

Allo stato attuale, mediante l'implementazione del presente manuale, Collegio Morigi recepisce **i profili di norma (provvedimenti / integrazioni / linee guida / interpretazioni) emanati dalle Autorità competenti a seguito dell'entrata in vigore del GDPR fino all'anno precedente a quello di emissione**, di seguito classificate:

ANNO	PROFILO DI NORMA	AUTORITA'	RECEPIMENTO *(se applicabile)*
2023	**Linee guida per la conservazione delle password (12/12/2023)** indicazioni sulle misure tecniche da adottare per garantire la sicurezza delle password, sviluppate con il supporto dell'agenzia per la cybersicurezza nazionale	Garante Italiano, ACN	*Verificata applicabilità delle linee guida al contesto del Titolare*
2023	**Intelligenza artificiale, indagine sull'utilizzo dei dati (22/11/2023)** istruttoria volta a verificare l'adozione di misure di sicurezza da parte di siti/servizi basati su IA	Garante Italiano	*Verificata applicabilità dell'indagine al contesto del Titolare*
2023	**Guida all'applicazione del GDPR (05/08/2023)** Nuova edizione di un manuale di sintesi degli adempimenti richiesti alle aziende	Garante Italiano	*Verificata aderenza del presente Modello con le indicazioni del Garante*
2023	**Data Privacy Framework (10/07/2023)** Nuovo accordo UE/USA per il flusso transnazionale di dati	Commissione Europea / USA	*Verificata applicabilità, con particolare riferimento a presenza on-line*
2023	**Linee Guida EDPB in materia di notifica di data breach (05/04/2023)** recepimento delle indicazioni del board EDPB nella procedura di notifica online del Garante Italiano	EDPB	*Indicazioni incluse in processo di gestione di eventuale data breach* https://servizi.gpdp.it/databreach/s/
2023	**D.Lgs. 24/2023 Decreto Whistleblowing (31/03/2023) e indicazioni operative Garante (28/12/2023)** obbligo di attivazione e gestione del canale di segnalazione e relativi adempimenti privacy	Governo Italiano	*Verificata applicabilità del Decreto e relativi adempimenti (nomine, informative, registro, PIA)*
2023	**Telemarketing – Approvato il Codice di condotta (24/03/2023)** misure specifiche per garantire la correttezza e la legittimità dei trattamenti di dati svolti lungo tutta la "filiera" del telemarketing.	Garante Italiano	*Verificata applicabilità del Codice al contesto del Titolare*
2023	**Parità di genere – Questionario del Garante per le PMI (16/03/2023)** volto ad analizzare il livello di consapevolezza e le implicazioni riguardo la protezione dei dati personali	Garante Italiano; Enti UE	*Verificata applicabilità della tematica al contesto del Titolare*
2022	**Cookie Wall** il Garante apre una serie di istruttorie per accertare la conformità di tali iniziative (subordinare l'accesso ai contenuti di un sito al consenso sull'uso di cookies di profilazione) con la normativa europea	Garante Italiano	*Verificata applicabilità dei provvedimenti al contesto del Titolare*

© Documento valido ed utilizzabile dal Titolare del trattamento esclusivamente a fini di conformità interna

ANNO	PROFILO DI NORMA	AUTORITA'	RECEPIMENTO *(se applicabile)*
2022	**Decreto trasparenza** (D. Lgs. 104/2022) che ha recepito nell'ordinamento italiano la Direttiva europea 2019/1152 relativa a condizioni di lavoro trasparenti e prevedibili, con la quale sono stati estesi in modo sostanziale gli obblighi dei datori di lavoro rispetto alle informazioni da fornire ai lavoratori	Governo Italiano;	*Verificata compatibilità delle prescrizioni di norma rispetto al modello di conformità privacy*
2022	**Telemarketing** Definitiva riorganizzazione del Registro delle opposizioni e nuove modalità per presentazione reclami	Governo Italiano; Garante Italiano	*Verificata applicabilità al contesto del Titolare*
2022	Garante privacy stop all'uso dei **Google Analytics**. Dati trasferiti negli Usa senza adeguate garanzie	Garante Italiano	*Verificata presenza on-line e prescrizioni del provvedimento*
2022	**Antivirus Kaspersky** Istruttoria del Garante per valutare i potenziali rischi relativi al trattamento dei dati personali dei clienti italiani effettuato dalla società russa che fornisce il software antivirus Kaspersky	Garante Italiano	*Verificata applicabilità e valutazione esiti istruttoria*
2022	**Riconoscimento facciale** Provvedimento sanzionatorio su società americana per violazione principi generali GDPR	Garante Italiano	*Verificata applicabilità del provvedimento al contesto del Titolare ed eventuali prescrizioni*
2022	**Codici di Condotta** Il Garante ha pubblicato il Registro dei codici di condotta, adempimento previsto dall'art. 40 paragrafo 6 del Regolamento (UE) 2016/679, ai sensi del quale ogni Autorità garante che approva un codice di condotta deve registrarlo e pubblicarlo.	Garante Italiano	*Verificata eventuale applicabilità dei codici di condotta al contesto del Titolare* www.gpdp.it/codici-di-condotta
2022	**Linee Guida Agid sulla conservazione digitale a norma** (in vigore da gennaio 2022) riorganizzazione della norma sui documenti elettronici e vincoli per una corretta conservazione: nomina responsabile, redazione manuale, piano di controlli	Agid Garante Italiano	*Verifica della corretta attribuzione dei ruoli previsti e della compilazione del registro dei trattamenti*
2021	Provvedimento 10/06/2021 "Linee guida **cookie** e altri strumenti di tracciamento" *(nuovo banner in relazione all'eventuale utilizzo di cookies di profilazione)*	Garante Italiano	*Adeguamento sito web in relazione alle prescrizioni normative*
2021	Vademecum "Suggerimenti per creare e gestire **password** a prova di privacy"	Garante Italiano	*Verifica coerenza delle proprie impostazioni rispetto ai suggerimenti dell'Autorità*
2021	Normativa **Green-Pass** e relativi pareri Autorità Garante *(DL 52 del 22/04/2021 "Misure urgenti per la graduale ripresa delle attività economiche e sociali nel rispetto delle esigenze di contenimento della diffusione dell'epidemia da COVID-19" e successive modifiche ed integrazioni)*	Governo Italiano; Garante Italiano	*Introduzione di procedure, modalità e strumenti di verifica coerenti con le prescrizioni di legge e con le relative pronunce del Garante*
2021	Nuove regole deontologiche in ambito statistico e codice di condotta sulle informazioni commerciali	Garante Italiano	*Verificata applicabilità delle regole*
2021	Linee di indirizzo del Garante Privacy sull'attività degli **RPD/DPO** *Faq sul Responsabile della Protezione dei Dati (RPD/DPO) in ambito private*	Garante Italiano	*Verificata applicabilità e coerenza delle linee guida al contesto dell'organizzazione*
2021	**Vaccinazioni sul luogo di lavoro** e ruolo del medico competente *(documento di indirizzo per il trattamento dei dati connessi all'adesione alla campagna vaccinale sui luoghi di lavoro – Protocollo nazionale 06/04/2021)*	Governo Italiano; Garante Italiano	*Valutata possibilità di adesione e (nel caso) applicate le misure*
2021	**Vaccinazioni dei dipendenti:** le FAQ del Garante Privacy *(indicazioni e principi generali per una corretta applicazione della disciplina sulla protezione dei dati)*	Garante Italiano	*Verificate ed applicate le indicazioni*
2021	Pareri congiunti su nuove **Clausole Contrattuali Tipo** proposte dalla Commissione Europea da parte *(aggiornamento delle clausole da utilizzarsi al fine di legittimare trasferimenti di dati extra UE e delle clausole da utilizzarsi per i contratti tra Titolari e Responsabili del trattamento)*	EDPB[(1)]; EDPS[(2)]	*Verificata applicabilità dei pareri e coerenza del proprio sistema di compliance*
2020	**Data Breach** *(nuovo servizio del Garante per supportare i titolari del trattamento negli adempimenti previsti in caso di Data Breach)*	Garante Italiano	*Verifica della coerenza tra le indicazioni fornite dal Garante e la procedura interna di cui al Capitolo 8 del presente manuale e moduli allegati)*

© Documento valido ed utilizzabile dal Titolare del trattamento esclusivamente a fini di conformità interna

ANNO	PROFILO DI NORMA	AUTORITA'	RECEPIMENTO *(se applicabile)*
2020	**Siti web e cookies** *(Avviso relativo alla consultazione sulle "Linee guida sull'utilizzo di cookie e di altri strumenti di tracciamento" - 10 dicembre 2020)*	Garante Italiano	*Verifica della coerenza del proprio sito web e relativa privacy policy con le indicazioni del Garante*
2020	**Videosorveglianza** *(le indicazioni del Garante privacy: le regole per installare ed utilizzare telecamere – 05 dicembre 2020)*	Garante Italiano	*Verifica della coerenza dei sistemi di videosorveglianza con le indicazioni del Garante (vedi registro trattamenti ed eventuali allegati dedicati)*
2020	**Fatturazione elettronica** *(Parere sullo schema di provvedimento del Direttore dell'Agenzia delle entrate concernente Regole tecniche per l'emissione e la ricezione delle fatture elettroniche per le cessioni di beni e le prestazioni di servizi effettuate tra soggetti residenti e stabiliti nel territorio dello Stato e per le relative variazioni - 9 luglio 2020)*	Garante Italiano	*Adozione di strumenti coerenti con gli obblighi di legge e procedure di compilazione adeguate rispetto ai criteri di pertinenza e minimizzazione dei dati*
2020	**Emergenza Coronavirus** *(indicazioni del Garante privacy su scuola, lavoro, sanità, ricerca ed enti locali. Chiarimenti e indicazioni per pubbliche amministrazioni e imprese private – 4 maggio 2020)*	Garante Italiano	*Adeguate le procedure di sicurezza alle indicazioni dei protocolli nazionali e dei dpcm applicabili (vedi registro trattamenti)*
2020	**Flussi di dati extra-UE Linee guida 2/2020 e raccomandazioni** *(il Comitato europeo per la protezione dei dati ha adottato raccomandazioni sulle misure che integrano gli strumenti di trasferimento dei dati per garantire il rispetto del livello UE di protezione dei dati personali, nonché raccomandazioni sulle cosiddette "garanzie essenziali europee" in rapporto alle misure di sorveglianza).*	EDPB	*Verifica di eventuali trasferimenti di dati extra UE e del relativo principio di legittimità (vedi registro trattamenti)*
2020	**Linee guida 5/2020 Consenso** *(indicazioni per acquisizione di un consenso valido)*	EDPB	*Verifica modalità e casistiche di acquisizione consenso (vedi informative allegate e registro trattamenti)*
2020	**Linee guida 3,4/2020 Emergenza sanitaria** *(trattamento dei dati relativi alla salute a fini di ricerca scientifica nel contesto dell'emergenza legata al COVID-19; uso dei dati di localizzazione e degli strumenti per il tracciamento dei contatti nel contesto dell'emergenza legata al COVID-19)*	EDPB	*Adeguate le procedure di sicurezza alle indicazioni dei protocolli nazionali e dei dpcm applicabili (vedi registro trattamenti)*
2019	Linee guida 2/2019 "trattamento dei dati personali nel contesto della fornitura di servizi on-line"	EDPB	*Verificata eventuale presenza on-line e connesse valutazioni su informativa e registro trattamenti*
2019	Raccomandazione 1/2019 "trattamenti soggetti all'obbligo di valutazione di impatto privacy"	EDPB	*Verificato registro trattamenti, in riferimento ai 9 criteri relativi alla PIA*
2019	Linee guida 3/2019 "trattamento dei dati tramite sistemi di videosorveglianza"	EDPB	*Verificata applicabilità e coerenza con i requisiti richiesti*
2019	Linee guida 4/2019 "criteri di valutazione della Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita"	EDPB	*Verificate attività censite nel registro dei trattamenti*
2019	Linee giuda 5/2019 "criteri di garanzia di esercizio del diritto all'oblio"	EDPB	*Verifica presenza di apposita modulistica per gestione delle richieste*
2019	Linee guida WP29 sulla gestione del consenso	WP Art.29 (3)	*Verificati trattamenti svolti sotto il principio di legittimità del consenso*
2019	Linee guida WP29 sulla gestione data breach	WP Art.29	*Verifica presenza di apposita modulistica per gestione violazioni dati personali*
2019	Linee guida WP29 sul registro dei trattamenti	WP Art.29	*Verificata presenza registro trattamenti*
2019	Tutorial del Garante sulla "individuazione e gestione del rischio"	Garante Italiano	*Verificata procedura e assegnazione rating*

(1) European Data Protection Board (Comitato della Autorità Garanti nazionali)

(2) European Data Protection Supervisor (Garante Europeo per la protezione dei dati)

(3) Working Party Art.29 (Gruppo di lavoro privacy europeo)

Definizioni

Tutti i termini utilizzati nel presente documento si rifanno alle definizioni di cui all'Art.4 del Reg.UE 2016/679.

© Documento valido ed utilizzabile dal Titolare del trattamento esclusivamente a fini di conformità interna

Elementi di contesto significativi per il sistema di conformità privacy

Il GDPR prevede che il Titolare ponga in essere misure di conformità pertinenti, adeguate e proporzionate rispetto al proprio **contesto operativo / organizzativo**. Di seguito si classificano pertanto gli elementi essenziali che contestualizzano l'attività di Collegio Morigi.

Descrizione	 L'ASP Collegio Morigi – De Cesaris è un'azienda di servizi alla persona costituita il 1 settembre 2008 dalla fusione di due storiche realtà piacentine, l'Opera Pia Collegio Maschile Morigi e la Fondazione De Cesaris – Nicelli – Cella – Ceruti. L'ASP ha personalità giuridica di diritto pubblico ed è dotata di autonomia statutaria, gestionale, patrimoniale, contabile e finanziaria e non ha fini di lucro. L'attività è incentrata nella gestione del collegio, nell'erogazione di borse di studio a favore di studenti delle scuole medie di primo e secondo grado e nel coordinamento del progetto di "Vicinato solidale". Il Collegio è membro dell'Associazione Collegi di Piacenza.
Missione e valori	Lo Statuto del Collegio approvato dalla Regione Emilia Romagna il 27 giugno 2008 riassume e rilancia le finalità degli enti originari che all'articolo 4 sono così descritte: L'ASP offre assistenza agli studenti universitari e a quelli delle scuole superiori tramite: a) erogazione di borse di studio agli studenti meritevoli ed altre provvidenze economiche a sostegno del successo formativo; b) supporto logistico, economico e socio-culturale. L'ASP ispira e orienta la propria attività al rispetto delle finalità e dei principi e in particolare: a) rispetto della dignità della persona; b) adeguatezza, flessibilità e personalizzazione degli interventi, nel rispetto delle opzioni dei destinatari e delle loro famiglie. Nello sviluppo delle norme statutarie il Collegio Morigi ha individuato nel suo Progetto formativo i capisaldi del percorso di crescita degli studenti ospiti: • superare una concezione egocentrica della vita, imparando a conoscere e accogliere l'altro, con la sua ricchezza, i suoi limiti e le sue necessità; • imparare a vivere come soggetto attivo in una comunità; • riconoscere i propri diritti e le proprie responsabilità; • compiere in autonomia scelte e saperle giustificare; • maturare un proprio stile di vita; • acquisire un senso di rispetto per i diversi ruoli di ciascun componente della comunità ed il significato della presenza di ognuno per il bene comune; • riconoscere il valore della norma (statuto e regolamento) come aiuto per la crescita ordinata della vita comunitaria; • acquisire il rispetto dei luoghi e delle strutture messe a disposizione. • imparare ad accettare e rispettare culture diverse da quelle delle proprie origini. Nel 2014 è stato approvato un nuovo statuto che prevede l'istituzione della figura del Amministratore unico in sostituzione del consiglio di amministrazione.
Statuto	https://www.collegiomorigi.it/wp-content/uploads/2021/01/STATUTO-approvato-23-giugno-2014.pdf
Ulteriori info	Su sito web www.collegiomorigi.it è possibile trovare ulteriori info, in merito a: - Servizi di ospitatlità - Storia del Collegio - Albo pretorio on-line - Galleria fotografica

© Documento valido ed utilizzabile dal Titolare del trattamento esclusivamente a fini di conformità interna

3) MODELLO DI CONFORMITA'

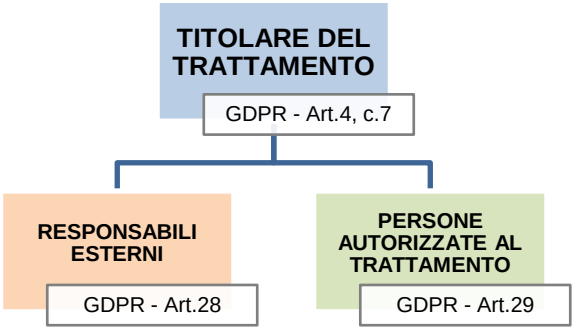
Il modello di conformità adottato da Collegio Morigi è finalizzato a fornire adeguate evidenze rispetto ai requisiti di legge previsti dal GDPR, secondo il seguente schema.

REQUISITO	RIF.GDPR	EVIDENZA NEL MANUALE	ALLEGATI
Definire ruoli e responsabilità dei soggetti coinvolti nel sistema	Art.26-29	Capitolo 4 ORGANIGRAMMA	• Nomina autorizzati • Nomina esterni
Mappare le attività di trattamento, valutando i rischi per gli interessati ed il relativo piano di sicurezza	Art.30-32	Capitolo 5 ACCOUNTABILITY	
Gestire eventuali incidenti di sicurezza	Art.33,34	Capitolo 6 DATA BREACH	• Data breach
Divulgare adeguate informazioni agli interessati	Art.12-14	Capitolo 7 INFORMATIVE	• Informativa (modelli vari)
Garantire i diritti degli interessati	Art.15-22	Capitolo 8 DIRITTI DEGLI INTERESSATI	• Diritti interessati
Gestire l'attuazione e l'aggiornamento del sistema	Art.24	Capitolo 9 GESTIONE SISTEMA CONFORMITA'	

© Documento valido ed utilizzabile dal Titolare del trattamento esclusivamente a fini di conformità interna

4) GOVERNANCE (Ruoli e responsabilità previsti dalla normativa)

Scopo del presente capitolo è **orientare la distribuzione dei compiti e delle responsabilità** nell'ambito dei soggetti preposti al trattamento dei dati, secondo le definizioni previste dal GDPR (vedi figura seguente).



Le seguenti tabelle identificano i suddetti soggetti:

Ruolo	**Titolare del trattamento**
Identificazione	Collegio Morigi, in persona del Legale Rappresentante, che esercita il potere decisionale su modalità e finalità del trattamento

Ruolo	**Responsabili esterni**
Identificazione	I fornitori/consulenti (aziende) esterni a cui viene commissionato un trattamento

Nome / Ragione sociale	**Servizio erogato**
ER.GO	Servizi di accoglienza universitaria
REAL CATERING SLEM	Servizi mensa del Collegio
MENTRONOTTE PIACENZA	Servizi di reception, guardiania, videosorveglianza
ZUCCHETTI	Servizi informatici

Ruolo	**Soggetti autorizzati**
Identificazione	I dipendenti/collaboratori (persone fisiche) che possono accedere a dati personali nell'espletamento dei loro incarichi

Cognome/Nome	**Mansione / Ufficio**
Vedi atti di designazione	

Modalità di designazione

Titolare	Non risulta necessaria alcuna designazione, in quanto il ruolo è predefinito a livello normativo.	
Responsabili esterni (Art.28)	- Contestualmente alla messa a norma verrà divulgato e sottoscritto l'accordo contrattuale di nomina; - In caso di nuovi consulenti verrà divulgato l'atto preliminarmente all'avvio del rapporto professionale. **GDPR-3-Nomina esterni**	Annualmente verrà effettuata una verifica dell'elenco e delle garanzie di compliance
Soggetti autorizzati (Art.29)	- Contestualmente alla messa a norma verrà divulgato e sottoscritto l'accordo contrattuale di nomina - In caso di nuovi assunti verrà divulgato l'atto preliminarmente all'avvio del rapporto professionale **GDPR-3-Nomina autorizzati**	Annualmente verrà effettuata una verifica dell'elenco

© Documento valido ed utilizzabile dal Titolare del trattamento esclusivamente a fini di conformità interna

Altre cariche

Data Protection Officer	◎	Il Titolare non è soggetto ai requisiti che prevedono la nomina e non ha provveduto su base volontaria
	◉	Il Titolare ha provveduto alla nomina del DPO
	GPDP.Ufficio.Registro RPD.0000682.23/01/2023  **Comunicazione dei dati di contatto del Responsabile della Protezione dei Dati - RPD** (art. 37, par. 7, RGPD e art. 28, c. 4 del D.Lgs. 51/2018)	
Contitolari del trattamento	◉	Non si effettuano trattamenti in ambito di contitolarità con altre organizzazioni
	◎	Si effettuano trattamenti in ambito di contitolarità con altre organizzazioni
Rappresentanti sul territorio UE	◉	Non si rientra nell’ambito di applicazione di nomina del Rappresentante
	◎	Si rientra nell’ambito di applicazione di nomina del Rappresentante
Ricezione di nomina a Resp.esterno da altro Titolare	Di norma Collegio Morigi non viene nominata quale Responsabile esterno da altri Titolari. Eventuali attività svolte in qualità di responsabile esterno (nominato da altro Titolare) saranno mappate nel registro dei trattamenti	

© Documento valido ed utilizzabile dal Titolare del trattamento esclusivamente a fini di conformità interna

5) ACCOUNTABILITY (Registro dei trattamenti, piano di sicurezza)

Il GDPR pone con forza l'accento sulla "**responsabilizzazione**" (accountability nell'accezione inglese) del Titolare, ossia sull'adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento (Artt. 23-25, in particolare, e l'intero Capo IV del regolamento). Si tratta di una grande novità per la protezione dei dati in quanto viene affidato ai titolari il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali, nel rispetto delle disposizioni normative e alla luce di alcuni criteri specifici indicati nel regolamento. Si richiede pertanto un'analisi preventiva e un impegno applicativo da parte dei titolari che devono sostanziarsi in una serie di **attività specifiche e dimostrabili (fasi del processo)**:

- registro trattamenti (mappatura delle attività di trattamento / banche dati, GDPR-Art.30)
- implementazione di adeguate misure di sicurezza (GDPR-Art.32)

5.1) Registro dei trattamenti

L'art. 30 del GDPR prevede tra gli adempimenti principali del titolare del trattamento la **tenuta del registro delle attività di trattamento**. E' una classificazione contenente le principali informazioni (specificatamente individuate dall'art. 30 del GDPR) relative alle operazioni di trattamento svolte dal titolare. Il Registro costituisce uno dei principali elementi di accountability del titolare, in quanto strumento idoneo a fornire un quadro aggiornato dei trattamenti in essere all'interno dell'organizzazione, indispensabile per ogni attività di valutazione o analisi del rischio e dunque preliminare rispetto a tali attività. Il registro ha forma scritta, anche elettronica, e viene esibito su richiesta al Garante. Il Registro è strutturato secondo le indicazioni dell'Art.30 del GDPR, nonché delle istruzioni in merito dell'Autorità Garante per la protezione dei dati personali.

REGISTRO DEI TRATTAMENTI

Dati di contatto
Titolare del trattamento: Collegio Morigi
Estremi di contatto indicati nelle informative: direzione@collegiomorigi.it – info@pec.collegiomorigi.it

DPO: Galli Data Service Srl
Estremi di contatto indicati nelle informative: dpo@gallidataservice.com – gallidataservicesrl@pec.it

Ultimo aggiornamento:
Data ultima modifica: vedi data emissione, in intestazione

Schede Registro > VEDI APPENDICE

Le schede del registro dei trattamenti sono disponibili in appendice al presente Modello.

© Documento valido ed utilizzabile dal Titolare del trattamento esclusivamente a fini di conformità interna

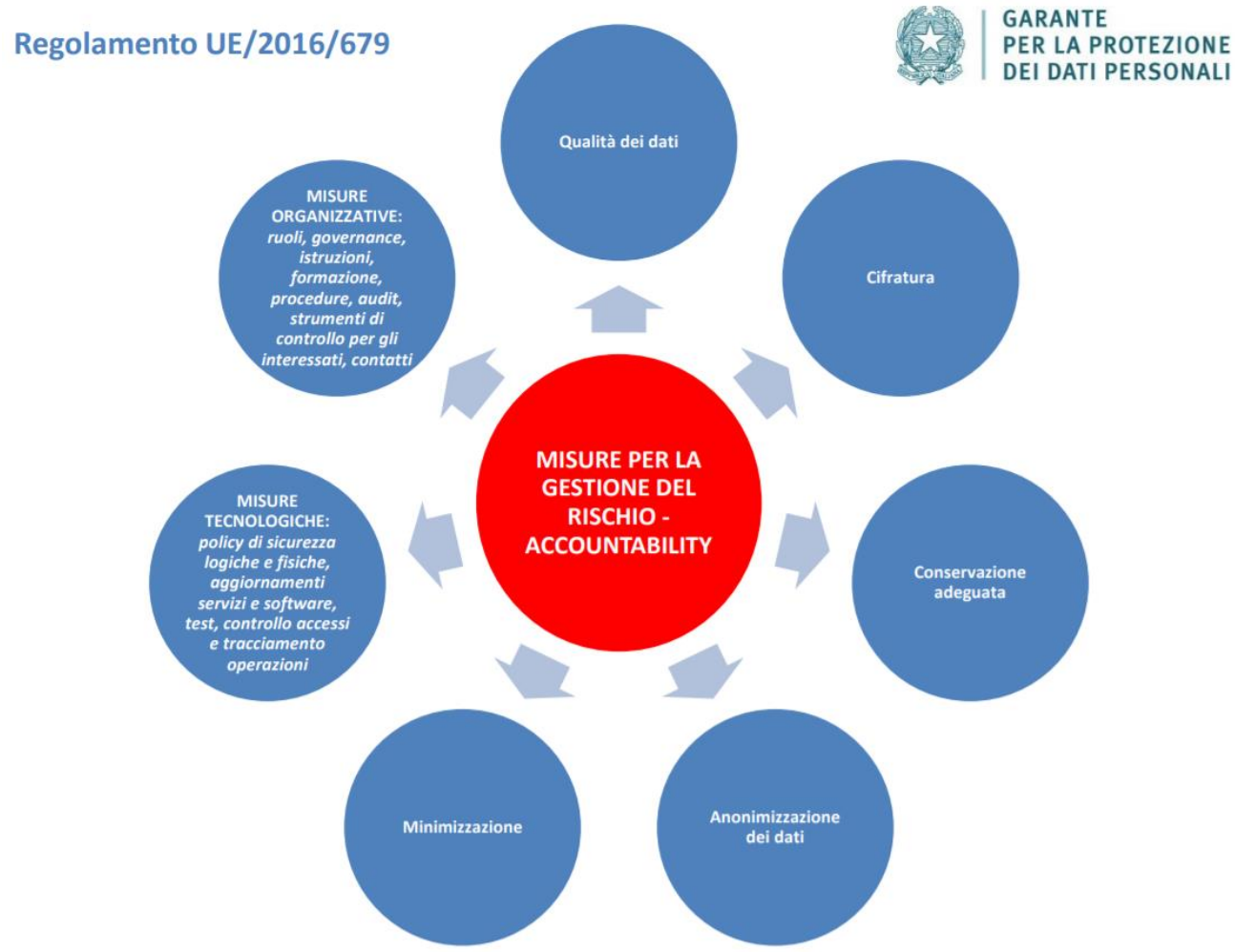
5.2) Piano di sicurezza

Nel GDPR l'implementazione di adeguate misure di sicurezza a tutela dei dati si colloca alla fine del processo di "responsabilizzazione". Le misure di sicurezza devono garantire un livello di sicurezza adeguato al rischio (art.32, par.1). Per tale motivo il GDPR fornisce una lista aperta non esaustiva. Per lo stesso motivo non possono sussistere dopo il 25/05/2018 obblighi generalizzati di adozione di "misure minime" di sicurezza, poiché tale valutazione è rimessa, caso per caso, al Titolare, in rapporto ai rischi specificatamente individuati.

Scelta delle misure di sicurezza adeguate

Nella scelta delle misure di sicurezza il Titolare adotta come riferimento gli obiettivi di controllo previsti dai principali standard di riferimento internazionali riferiti alla sicurezza dei dati (*ISO 27001*), nonché le linee guida formulate dall'ENISA (*Guidelines for SMEs on the security of personal data processing*).

Si tiene conto infine delle indicazioni dell'Autorità Garante, di cui si riporta abstract



Le misure di sicurezza sono:

- indicate nelle apposite righe del registro dei trattamenti;
- inserite in apposito disciplinare interno, riportato in Appendice 2.

© Documento valido ed utilizzabile dal Titolare del trattamento esclusivamente a fini di conformità interna

6) DATA BREACH (Violazioni dei dati personali)

DEFINIZIONE

Si ha una "violazione dei dati personali" quando accidentalmente (colposamente) o in modo illecito (dolosamente) un evento causa la distruzione, la perdita, la modifica, la divulgazione non autorizzata, l'accesso ai dati personali trasmessi, conservati o comunque trattati. (es: furto di strumenti/documenti; smarrimento di strumenti/documenti; azione di virus informatico o attacco hacker; cancellazione/divulgazione involontaria, ecc.).

OBBLIGHI

Collegio Morigi è tenuta a documentare le violazioni di dati personali subite, nonché le relative circostanze e conseguenze e i provvedimenti adottati (tramite un registro interno). Il GDPR prevede inoltre l'obbligo di notificare all'autorità di controllo le violazioni di dati personali di cui vengano a conoscenza, entro 72 ore e comunque "senza ingiustificato ritardo", ma soltanto se ritengono probabile che da tale violazione derivino rischi per i diritti e le libertà degli interessati (GDPR, considerando 85). Qualora il livello di rischio risultasse elevato occorre procedere alla notifica agli interessati.

NOTE OPERATIVE / PROCEDURA, AL FINE DI PRESIDIARE LA GESTIONE DEI DATA BREACH

- i soggetti **Autorizzati** (se presenti) sono tenuti a segnalare al **Titolare**, o ad eventuali coordinatori privacy, qualsiasi evento assimilabile alla definizione di data breach (sensibilizzazione tramite lettere di designazione ed istruzioni)

- i **Responsabili esterni** (se presenti) sono tenuti a segnalare al **Titolare**, o ad eventuali coordinatori privacy, qualsiasi evento assimilabile alla definizione di data breach (sensibilizzazione tramite lettere di designazione ed istruzioni)

- il **Titolare** valuterà (con il supporto di eventuali consulenti/coordinatori privacy) la portata dell'evento ed il livello di rischio residuo;

- il **Titolare** si occuperà (con il supporto di eventuali consulenti/coordinatori privacy) della compilazione del registro; **GDPR-2-Data breach**

- il **Titolare** si occuperà (con il supporto di eventuali consulenti/coordinatori privacy), qualora necessario, della segnalazione all'Autorità Garante / Interessati; **GDPR-2-Data breach** e tools di supporto sul portale dell'Autorità Garante

☑ **ADEMPIMENTI DATA BREACH GESTITI**

© Documento valido ed utilizzabile dal Titolare del trattamento esclusivamente a fini di conformità interna

7) INFORMATIVA (Informazioni da fornire agli interessati)

Il GDPR prevede che il Titolare del trattamento adotti misure appropriate per fornire all'interessato (tutti i soggetti di cui si acquisiscono dati personali) tutte le informazioni di cui agli articoli 13 e 14 (informative) in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro. Il GDPR prevede che tali informazioni siano fornite per iscritto o con altri mezzi, anche, se del caso, con mezzi elettronici.

Il GDPR richiede inoltre che, in taluni casi, venga richiesto uno specifico consenso agli interessati. Non risulta necessario acquisire un consenso nei seguenti casi:

- il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
- il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;
- il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;
- il trattamento è necessario per l'esecuzione di un COMPITO DI INTERESSE PUBBLICO o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;
- il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato, in particolare se l'interessato è un minore.

La seguente tabella riporta l'elenco delle informative utilizzate da Collegio Morigi e le relative modalità attuative.

INFORMATIVA IN USO	MODALITA' ATTUATIVE / DIVULGATIVE
Informativa generale	Pubblicata su sito web aziendale o messa a disposizione su richiesta (contiene riferimento sito, cookies e client/fornitori)
Informativa lavoratori	Consegnata in occasione dell'entrata in servizio o in caso di significative variazioni
Informativa email	Inserita in calce ad ogni email in uscita
Informativa foto/video	Consegnata al momento della produzione di contenuti foto/video

© Documento valido ed utilizzabile dal Titolare del trattamento esclusivamente a fini di conformità interna

8) DIRITTI DEGLI INTERESSATI

I diritti che l'interessato può esercitare nei confronti del Titolare del trattamento che gestisce i suoi dati sono definiti agli Art.15-22 del GDPR:

DIRITTO	DESCRIZIONE
Art.15 Diritto di accesso	L'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e alle informazioni generali del trattamento
Art.16 Diritto di rettifica	L'interessato ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo
Art.17 Diritto di cancellazione (oblio)	L'interessato ha il diritto di ottenere dal titolare del trattamento, in presenza di giustificati motivi ed in coerenza con adempimenti di legge, la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo
Art.18 Diritto di limitazione	L'interessato, al ricorrere di talune ipotesi, ha il diritto di ottenere dal titolare del trattamento la limitazione del trattamento
Art.20 Diritto alla portabilità	L'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti
Art.21 Diritto di opposizione	L'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano
Art.22 Processi decisionali automatizzati (profilazione)	L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona.

NOTE OPERATIVE / PROCEDURA, AL FINE DI PRESIDIARE EVENTUALI RICHIESTE DEGLI INTERESSATI

- gli **Autorizzati** (se presenti) sono tenuti a segnalare al **Titolare**, o ad eventuali coordinatori privacy, qualsiasi richiesta in materia di privacy che dovesse pervenirgli in qualsiasi modo da qualsiasi soggetto (sensibilizzazione tramite lettere di designazione ed istruzioni)
- i **Responsabili esterni** (se presenti) sono tenuti a segnalare al **Titolare**, o ad eventuali coordinatori privacy, qualsiasi richiesta che dovesse loro pervenire in materia di diritti degli interessati rispetto a trattamenti svolti (sensibilizzazione tramite lettere di designazione ed istruzioni)
- gli **Autorizzati** (se presenti) sono tenuti a comunicare all'interessato che la richiesta verrà presa in carico dal **Titolare** per fornire un'adeguata risposta nei termini di legge (qualora non disponibile gli autorizzati dovranno richiedere un recapito del richiedente)
- il **Titolare** valuterà (con il supporto di eventuali consulenti/coordinatori privacy) la corretta identificazione del richiedente e la portata delle richieste;
- il **Titolare** organizza ordinatamente le banche dati, al fine di consentire un'agevole consultazione (propedeutica ad una tempestiva ed esaustiva risposta agli interessati)
- il **Titolare** si occuperà (con il supporto di eventuali consulenti/coordinatori privacy) di gestire la richiesta tramite l'apposita modulistica allegata, che consentirà di: tracciare la richiesta (MOD.1); valutarne l'evasione (MOD.2); rispondere al richiedente (MOD.3) **GDPR-3-Diritti interessati**

☑ **DIRITTI DEGLI INTERESSATI GARANTITI**

© Documento valido ed utilizzabile dal Titolare del trattamento esclusivamente a fini di conformità interna

9) GESTIONE SISTEMA DI CONFORMITA'

Il sistema di conformità privacy di Collegio Morigi è gestito (attuato, mantenuto, verificato ed aggiornato) tramite le seguenti modalità.

Gestione documentale	**Conservazione documenti**	◉ Su piattaforma digitale sicura (Datacenter certificato ISO 27.001 e protocolli di trasmissione dati muniti di SSL) ◉ Presso sede Titolare in formato cartaceo ◎ Presso sede Titolare in formato elettronico
	Validazione documenti	◉ Sottoscrizione Modello privacy in formato cartaceo originale ◉ Validazione documentazione allegata tramite tool digitale basato su casella email personale e riservata
	Aggiornamento ed attuazione documenti	I contenuti del modello privacy saranno oggetto di aggiornamento su base annuale, fornendo una classificazione dei parametri alla data di revisione del documento. In corso d'anno, saranno altresì oggetto di aggiornamento immediato: • modulo registro violazioni (in caso di data breach) • moduli diritti interessati (in caso di richiesta) • registro trattamenti (in caso di nuova attività di trattamento dati personali) • nomina autorizzati e nomina esterni (in caso di nuovi soggetti) • informative (in caso di variazioni significative dei contenuti o processi)
	Validità del modello	Il presente modello è valido fino alla successiva riemissione, da effettuarsi entro il termine dell'anno successivo alla data del presente documento. Annualmente verrà infatti riemesso il modello al fine di aggiornarlo allo scenario normativo di riferimento ed alle variazioni nell'assetto organizzativo del Titolare (ottemperando altresì ai requisiti di verifica periodica previsti dal GDPR). I moduli allegati potranno essere confermati nella validità, previa valutazione dello scenario di legge.
	Documentazione pregressa	Ai sensi delle significative novità introdotte dal GDPR il Titolare ha deciso di effettuare una revisione complessiva della compliance privacy, pertanto il presente modello e relativi allegati annullano e sostituiscono la documentazione precedentemente adottata
	Divulgazione	Il presente modello e moduli allegati non devono essere oggetto di divulgazione. Essi potranno comunque essere esibiti, per certificare il sistema di conformità, ad autorità ispettive o organi di controllo.

© Documento valido ed utilizzabile dal Titolare del trattamento esclusivamente a fini di conformità interna

Gestione nomine ed istruzioni	**Nomina autorizzati**	◉ Contestuale all'entrata in servizio ◉ Conservazione nomine cartacee in fascicolo ◎ Validazione tool digitale basato su casella mail personale e riservata
	Formazione autorizzati	◉ Tramite divulgazione annuale istruzioni cartacee ◎ Tramite formazione in aula ◎ Tramite piattaforma FAD dedicata
	Nomina e monitoraggio esterni	◉ Nomine responsabili esterni contestuale all'avvio del rapporto ◉ Conservazione nomine cartacee in fascicolo ◎ Validazione tool digitale, basato su casella mail personale e riservata ◉ Monitoraggio annuale tramite contatto via email

Gestione eventi	**Gestione eventi DATA BREACH**	◉ Segnalazione data breach tramite tool piattaforma ◉ Presa in carico, monitoraggio e risoluzione tramite piattaforma e supporto consulente ◉ Reminder data breach e tracciatura processo tramite piattaforma
	Gestione eventi DIRITTI INTERESSATI	◉ Segnalazione richieste esercizio diritti degli interessati tramite tool piattaforma ◉ Presa in carico, monitoraggio e risoluzione tramite piattaforma e supporto consulente ◉ Reminder e tracciatura processo tramite piattaforma
	Gestione eventi NUOVI TRATTAMENTI	◉ Segnalazione nuovi trattamenti tramite tool piattaforma ◉ Presa in carico, monitoraggio e risoluzione tramite piattaforma e supporto consulente ◉ Reminder e tracciatura processo tramite piattaforma

Misure di sicurezza	◉ Le misure di sicurezza risultano adeguate rispetto al contesto, alla natura dei trattamenti, ai costi di attuazione, ai rischi per gli interessati ed ai data breach intercorsi ◎ Le misure di sicurezza devono essere oggetto di implementazione / sviluppo / perfezionamento

Valutazione complessiva	Il sistema di conformità di Collegio Morigi risulta: • completo a livello di documentazione; • effettivo ed aggiornato rispetto ai trattamenti effettuati; • compreso ed applicato dai soggetti preposti ai trattamenti; • attuato operativamente rispetto alle misure di sicurezza indicate.

© Documento valido ed utilizzabile dal Titolare del trattamento esclusivamente a fini di conformità interna

APPENDICE 1: SCHEDE REGISTRO TRATTAMENTI

	Trattamento			DATI PERSONALI			INTERESSATI		DESTINATARI	TRASFERIMENTI	SICUREZZA
AREA FUNZIONALE	Descrizione	Finalità	Contitolare (eventuale rappresentante)	Categoria	Dati Sensibili	Termine ultimo cancellazione	Categorie	Consenso	Categoria	Paesi Terzi Organismi inter.	Misure tecniche ed organizzative adottate
Personale		Trattamento dei dati finalizzato alla gestione degli adempimenti derivanti dal o connessi al rapporto di lavoro (compresi gli adempimenti in materia di igiene e sicurezza sul lavoro)		Personali Particolari (stato di salute, appartenenza ai sindacati)	SI	Dati conservati per 10 anni dalla cessazione del rapporto di lavoro	Dipendenti e loro famigliari (certificati, giustificativi di assenza)	SI	Soggetti che possono accedere ai dati in forza di disposizione di legge, di regolamento o di normativa comunitaria, nei limiti previsti da tali norme; Il personale dipendente, purché sia precedentemente qualificato come Responsabile o Autorizzato del trattamento, ovvero come Amministratore di Sistema; Soggetti che svolgono in totale autonomia come distinti Titolari del trattamento, ovvero in qualità di Responsabili esterni del trattamento all'uopo nominati, finalità ausiliarie alle attività e ai servizi del Collegio, centri di servizio, società o consulenti incaricati di fornire servizi, nei limiti delle finalità per le quali i dati sono stati raccolti.	NO	porte dotate di serrature, accesso nei locali di Direzione e Amministrazione consentito solo agli autorizzati, armadi dotati di chiave, inferriate alle finestre, impianto di allarme, incarichi scritti agli autorizzati al trattamento ed ai Designati con funzioni privacy, policy privacy e policy informatica scritta, percorso di formazione, accessi ai pc protetti da password, accessi autenticati, antivirus, procedure di backup, procedure di modifica password
Personale		Trattamento dei dati personali presenti all'interno delle buste paga		Personali Particolari (stato di salute appartenenza ai sindacati)	SI	Dati conservati per 10 anni dalla cessazione del rapporto di lavoro	Dipendenti, e loro famigliari (cettificati, giustificativi di assenza)	SI	Soggetti che possono accedere ai dati in forza di disposizione di legge, di regolamento o di normativa comunitaria, nei limiti previsti da tali norme; Il personale dipendente, purché sia precedentemente qualificato come Responsabile o Autorizzato	NO	porte dotate di serrature, accesso nei locali di Direzione e Amministrazione consentito solo agli autorizzati, armadi dotati di chiave, inferriate alle finestre, impianto di allarme, incarichi scritti agli autorizzati

© Documento valido ed utilizzabile dal Titolare del trattamento esclusivamente a fini di conformità interna

									del trattamento, ovvero come Amministratore di Sistema; Soggetti che svolgono in totale autonomia come distinti Titolari del trattamento, ovvero in qualità di Responsabili esterni del trattamento all'uopo nominati, finalità ausiliarie alle attività ed ai servizi del Collegio, società o consulenti incaricati di fornire servizi, nei limiti delle finalità per le quali i dati sono stati raccolti.		al trattamento ed ai Designati con funzioni privacy, policy privacy e policy informatica scritta, percorso di formazione, accessi ai pc protetti da password, accessi autenticati, antivirus, procedure di backup, procedure di modifica password
Personale		Trattamento dei dati finalizzato all'attività di formazione del personale		Personali	NO	Dati conservati per 10 anni dalla cessazione del rapporto di lavoro	Dipendenti, Docenti.	SI	Soggetti che possono accedere ai dati in forza di disposizione di legge, di regolamento o di normativa comunitaria, nei limiti previsti da tali norme; Il personale dipendente, purché sia precedentemente qualificato come Responsabile o Autorizzato del trattamento, ovvero come Amministratore di Sistema; Soggetti che svolgono in totale autonomia come distinti Titolari del trattamento, ovvero in qualità di Responsabili esterni del trattamento all'uopo nominati, finalità ausiliarie alle attività e ai servizi del Collegio, centri di servizio, società o consulenti incaricati di fornire servizi (es. formazione) nei limiti delle finalità per le quali i dati sono stati raccolti.	NO	porte dotate di serrature, accesso nei locali di Direzione e Amministrazione consentito solo agli autorizzati, armadi dotati di chiave, inferriate alle finestre, impianto di allarme, incarichi scritti agli autorizzati al trattamento ed ai Designati con funzioni privacy, policy privacy e policy informatica scritta, percorso di formazione, accessi ai pc protetti da password, accessi autenticati, antivirus, procedure di backup, procedure di modifica password

© Documento valido ed utilizzabile dal Titolare del trattamento esclusivamente a fini di conformità interna

Personale		Trattamento dei dati finalizzato alla gestione di tutti gli adempimenti derivanti o connessi alla cessazione del rapporto di lavoro in caso di decesso del dipendente		Personali Particolari (stato di salute)	SI	Dati conservati per 10 anni dalla cessazione del rapporto di lavoro	Dipendenti Familiari/eredi	SI	Soggetti che possono accedere ai dati in forza di disposizione di legge, di regolamento o di normativa comunitaria, nei limiti previsti da tali norme; Il personale dipendente, purché sia precedentemente qualificato come Responsabile o Autorizzato del trattamento, ovvero come Amministratore di Sistema; Soggetti che svolgono in totale autonomia come distinti Titolari del trattamento, ovvero in qualità di Responsabili esterni del trattamento all'uopo nominati società o consulenti incaricati di fornire servizi, nei limiti delle finalità per le quali i dati sono stati raccolti.	NO	porte dotate di serrature, accesso nei locali di Direzione e Amministrazione consentito solo agli autorizzati, armadi dotati di chiave, inferriate alle finestre, impianto di allarme, incarichi scritti agli autorizzati al trattamento ed ai Designati con funzioni privacy, policy privacy e policy informatica scritta, percorso di formazione, accessi ai pc protetti da password, accessi autenticati, antivirus, procedure di backup, procedure di modifica password
Personale		Trattamento dei dati consente alla ricezione CV cartacei e finalizzato alla selezione del personale		Personali Particolari	SI	Dati conservati per 1 anno	Candidati	SI	nessuno	NO	porte dotate di serrature, accesso nei locali di Direzione e Amministrazione consentito solo agli autorizzati, armadi dotati di chiave, inferriate alle finestre, impianto di allarme, incarichi scritti agli autorizzati al trattamento ed ai Designati con funzioni privacy, policy privacy e policy informatica scritta, percorso di formazione, accessi ai pc protetti da password, accessi autenticati, antivirus,

© Documento valido ed utilizzabile dal Titolare del trattamento esclusivamente a fini di conformità interna

											procedure di backup, procedure di modifica password
Amministrazione		Trattamento dei dati finalizzato alla gestione dell'anagrafica dei soggetti terzi che hanno accesso ai locali del Collegio (servizi di pulizia affidati ad esterni)		Personali	NO	Dati conservati per 1 anno dall'accesso presso la struttura	Dipendenti di imprese terze		Soggetti che possono accedere ai dati in forza di disposizione di legge, di regolamento o di normativa comunitaria, nei limiti previsti da tali norme; Il personale dipendente, purché sia precedentemente qualificato come Responsabile o Autorizzato del trattamento, ovvero come Amministratore di Sistema; Soggetti che svolgono in totale autonomia come distinti Titolari del trattamento, ovvero in qualità di Responsabili esterni del trattamento all'uopo nominati, finalità ausiliarie alle attività ed ai servizi del Collegio, società o consulenti incaricati di fornire servizi, nei limiti delle finalità per le quali i dati sono stati raccolti.	NO	porte dotate di serrature, accesso nei locali di Direzione e Amministrazione consentito solo agli autorizzati, armadi dotati di chiave, inferriate alle finestre, impianto di allarme, incarichi scritti agli autorizzati al trattamento ed ai Designati con funzioni privacy, policy privacy e policy informatica scritta, percorso di formazione, accessi ai pc protetti da password, accessi autenticati, antivirus, procedure di backup, procedure di modifica password
Personale		Attività di videosorveglianza finalizzata a tutelare il patrimonio e la sicurezza delle persone		Personali	NO	24 ore	Dipendenti Utenti - Terzi		Soggetti che possono accedere ai dati in forza di disposizione di legge, di regolamento o di normativa comunitaria, nei limiti previsti da tali norme; Soggetti che svolgono in totale autonomia come distinti Titolari del trattamento, ovvero in qualità di Responsabili esterni del trattamento all'uopo nominati, finalità ausiliarie alle attività e ai servizi della cooperativa,	NO	porte dotate di serrature, accesso nei locali di Direzione e Amministrazione consentito solo agli autorizzati, armadi dotati di chiave, inferriate alle finestre, impianto di allarme, incarichi scritti agli autorizzati al trattamento ed ai Designati con funzioni privacy, policy privacy e policy informatica

© Documento valido ed utilizzabile dal Titolare del trattamento esclusivamente a fini di conformità interna

									società o consulenti incaricati di fornire servizi, nei limiti delle finalità per le quali i dati sono stati raccolti (es. IVRI)		scritta, percorso di formazione, accessi ai pc protetti da password, accessi autenticati, antivirus, procedure di backup, procedure di modifica password
Personale		Trattamento dei dati finalizzato alla gestione polizze assicurative RC		Personali	SI		Dipendenti		Soggetti che possono accedere ai dati in forza di disposizione di legge, di regolamento o di normativa comunitaria, nei limiti previsti da tali norme; Il personale dipendente, purché sia precedentemente qualificato come Responsabile o Autorizzato del trattamento, ovvero come Amministratore di Sistema; Le società controllate, controllanti o comunque collegate ai sensi dell'articolo 2359 del codice civile esclusivamente per le finalità amministrativocontabili; Soggetti che svolgono in totale autonomia come distinti Titolari del trattamento, ovvero in qualità di Responsabili esterni del trattamento all'uopo nominati, finalità ausiliarie alle attività e ai servizi della cooperativa, le società controllate, controllanti o comunque collegate ai sensi dell'articolo 2359 del codice civile per fini ulteriori rispetto a quelli	NO	porte dotate di serrature, accesso nei locali di Direzione e Amministrazione consentito solo agli autorizzati, armadi dotati di chiave, inferriate alle finestre, impianto di allarme, incarichi scritti agli autorizzati al trattamento ed ai Designati con funzioni privacy, policy privacy e policy informatica scritta, percorso di formazione, accessi ai pc protetti da password, accessi autenticati, antivirus, procedure di backup, procedure di modifica password

© Documento valido ed utilizzabile dal Titolare del trattamento esclusivamente a fini di conformità interna

									amministrativocontabili, centri di servizio, società o consulenti incaricati di fornire servizi, nei limiti delle finalità per le quali i dati sono stati raccolti.		
Area Amministrativa		Trattamento dei dati finalizzato alla gestione di reclami e segnalazioni Trattamento dei dati finalizzato alla gestione delle operazioni necessarie e propedeutiche all'applicazione di rimborsi		Personali Particolari (stato di salute)	SI	Dati conservati per 10 anni dalla pratica di rimborso	Utenti (studenti ospitati)i, Dipendenti		Soggetti che possono accedere ai dati in forza di disposizione di legge, di regolamento o di normativa comunitaria, nei limiti previsti da tali norme; Il personale dipendente, purché sia precedentemente qualificato come Responsabile o Autorizzato del trattamento, ovvero come Amministratore di Sistema; Le società controllate, controllanti o comunque collegate ai sensi dell’articolo 2359 del codice civile esclusivamente per le finalità amministrativocontabili; Soggetti che svolgono in totale autonomia come distinti Titolari del trattamento, ovvero in qualità di Responsabili esterni del trattamento all’uopo nominati, finalità ausiliarie alle attività e ai servizi della cooperativa, le società controllate, controllanti o comunque collegate ai sensi dell’articolo 2359 del codice civile per fini ulteriori rispetto a quelli amministrativocontabili, centri di servizio, società o	NO	porte dotate di serrature, accesso nei locali di Direzione e Amministrazione consentito solo agli autorizzati, armadi dotati di chiave, inferriate alle finestre, impianto di allarme, incarichi scritti agli autorizzati al trattamento ed ai Designati con funzioni privacy, policy privacy e policy informatica scritta, percorso di formazione, accessi ai pc protetti da password, accessi autenticati, antivirus, procedure di backup, procedure di modifica password

© Documento valido ed utilizzabile dal Titolare del trattamento esclusivamente a fini di conformità interna

									consulenti incaricati di fornire servizi, nei limiti delle finalità per le quali i dati sono stati raccolti.		
Area Amministrativa		Trattamento dei dati finalizzato alla gestione e compilazione dell'anagrafica clienti, della contabilità e dell'amministrazione		Personali, Particolari (stato di salute)	SI	10 anni fiscali	Utenti (studenti ospitati), Fornitori, Dipendenti		Soggetti che possono accedere ai dati in forza di disposizione di legge, di regolamento o di normativa comunitaria, nei limiti previsti da tali norme; Il personale dipendente, purché sia precedentemente qualificato come Responsabile o Autorizzato del trattamento, ovvero come Amministratore di Sistema; Soggetti che svolgono in totale autonomia come distinti Titolari del trattamento, ovvero in qualità di Responsabili esterni del trattamento all’uopo nominati, finalità ausiliarie alle attività e ai servizi del Collegio, società o consulenti incaricati di fornire servizi, nei limiti delle finalità per le quali i dati sono stati raccolti.	NO	porte dotate di serrature, accesso nei locali di Direzione e Amministrazione consentito solo agli autorizzati, armadi dotati di chiave, inferriate alle finestre, impianto di allarme, incarichi scritti agli autorizzati al trattamento ed ai Designati con funzioni privacy, policy privacy e policy informatica scritta, percorso di formazione, accessi ai pc protetti da password, accessi autenticati, antivirus, procedure di backup, procedure di modifica password
Area Amministrativa		Trattamento dei dati finalizzato alla resa del servizio (ospitalità alberghiera)		Personali, Particolari (stato di salute, convinzioni religiose)	SI	Dati conservati per 10 anni dalla cessazione del rapporto contrattuale	Utenti (studenti ospitati e loro famigliari)	SI	Soggetti che possono accedere ai dati in forza di disposizione di legge, di regolamento o di normativa comunitaria, nei limiti previsti da tali norme (organismi di pubblica sicurezza, Prefettura) Il personale dipendente, purché sia precedentemente qualificato come Responsabile o Autorizzato del trattamento, ovvero	NO	porte dotate di serrature, accesso nei locali di Direzione e Amministrazione consentito solo agli autorizzati, armadi dotati di chiave, inferriate alle finestre, impianto di allarme, incarichi scritti agli autorizzati al trattamento ed ai Designati con funzioni privacy, policy privacy

© Documento valido ed utilizzabile dal Titolare del trattamento esclusivamente a fini di conformità interna

									come Amministratore di Sistema; Soggetti che svolgono in totale autonomia come distinti Titolari del trattamento, ovvero in qualità di Responsabili esterni del trattamento all'uopo nominati finalità ausiliarie alle attività ed ai servizi del Collegio, società o consulenti incaricati di fornire servizi, nei limiti delle finalità per le quali i dati sono stati raccolti.		e policy informatica scritta, percorso di formazione, accessi ai pc protetti da password, accessi autenticati, antivirus, procedure di backup, procedure di modifica password
Area Amministrativa		Trattamento finalizzato alla raccolta e gestione per riprese di video e foto per finalità di descrizione e promozione delle attività svolte dal Collegio		Personali	NO	Nel rispetto del principio di minimizzazione per il tempo corrente rsipetto alla finalità per la quale il dato è stato raccolto	Dipendenti, Utenti (studenti ospitati), terzi	SI	Soggetti che possono accedere ai dati in forza di disposizione di legge, di regolamento o di normativa comunitaria, nei limiti previsti da tali norme; Il personale dipendente, purché sia precedentemente qualificato come Responsabile o Autorizzato del trattamento, ovvero come Amministratore di Sistema; Giornali, Comuni, Università, altri enti pubblici e privati. Soggetti che svolgono in totale autonomia come distinti Titolari del trattamento, ovvero in qualità di Responsabili esterni del trattamento all'uopo nominati finalità ausiliarie alle attività ed ai servizi del Collegio,società o consulenti incaricati di fornire servizi, nei limiti	NO	porte dotate di serrature, accesso nei locali di Direzione e Amministrazione consentito solo agli autorizzati, armadi dotati di chiave, inferriate alle finestre, impianto di allarme, incarichi scritti agli autorizzati al trattamento ed ai Designati con funzioni privacy, policy privacy e policy informatica scritta, percorso di formazione, accessi ai pc protetti da password, accessi autenticati, antivirus, procedure di backup, procedure di modifica password

© Documento valido ed utilizzabile dal Titolare del trattamento esclusivamente a fini di conformità interna

									delle finalità per le quali i dati sono stati raccolti.		
Area Amministrativa		Trattamento finalizzato alla istruzione di pratiche di rimborso, assegnazione alloggi, contributi		Personali, Particolari (stato di salute)	SI	10 anni dalla gestione della pratica	Utenti (studenti ospitati), terzi	SI	Soggetti che possono accedere ai dati in forza di disposizione di legge, di regolamento o di normativa comunitaria, nei limiti previsti da tali norme (Enti pubblici e di pubblica sicurezza, Università, Comuni e altre p.a., Prefettura, Acer) Il personale dipendente, purché sia precedentemente qualificato come Responsabile o Autorizzato del trattamento, ovvero come Amministratore di Sistema; Soggetti che svolgono in totale autonomia come distinti Titolari del trattamento, ovvero in qualità di Responsabili esterni del trattamento all'uopo nominati, finalità ausiliarie alle attività ed ai servizi del Collegio, società o consulenti incaricati di fornire servizi, nei limiti delle finalità per le quali i dati sono stati raccolti.	NO	porte dotate di serrature, accesso nei locali di Direzione e Amministrazione consentito solo agli autorizzati, armadi dotati di chiave, inferriate alle finestre, impianto di allarme, incarichi scritti agli autorizzati al trattamento ed ai Designati con funzioni privacy, policy privacy e policy informatica scritta, percorso di formazione, accessi ai pc protetti da password, accessi autenticati, antivirus, procedure di backup, procedure di modifica password

© Documento valido ed utilizzabile dal Titolare del trattamento esclusivamente a fini di conformità interna

APPENDICE 2: POLICY SULLA SICUREZZA INFORMATICA

Si riporta, di seguito, un abstract della policy in oggetto

Azienda di **S**ervizi alla **P**ersona
Collegio Morigi – De Cesaris
Sede legale ed amministrativa: Piacenza – via Taverna 37
Codice Fiscale e P. I. 01531860334
Telefono 0523/338551 Fax 0523/320070
PEC: info@pec.collegiomorigi.it

POLICY SULLA SICUREZZA INFORMATICA
Disposizioni, regole di comportamento e misure organizzative
per il corretto utilizzo degli strumenti digitali aziendali
e per la prevenzione dei reati informatici

Introduzione
Il presente regolamento (di seguito anche solo "Policy") è adottato da:

► A.S.P. COLLEGIO MORIGI - DE CESARIS con sede legale in 29121 – Piacenza, via Via Taverna, n. 37, C.F./P.I. 01531860334, in persona di Eugenio Silva, nella qualità di Titolare del trattamento (in seguito "Titolare" o "ASP").

per disciplinare il corretto comportamento e utilizzo degli strumenti digitali aziendali al fine di prevenire la commissione – nell'interesse o a vantaggio della stessa – di talune condotte.

Attraverso la Policy vengono così definite le regole tecniche ed organizzative da applicare e rispettare, nonché quelle per l'utilizzo della posta elettronica e per la navigazione in internet da parte dei dipendenti e/o collaboratori e dell' ASP nell'ambito dello svolgimento delle loro mansioni.

La progressiva diffusione delle nuove tecnologie informatiche, le maggiori possibilità di interconnessione tra computer e l'aumento di informazioni trattate con strumenti elettronici aumentano, infatti, i rischi legati alla sicurezza e all'integrità delle informazioni, oltre alle conseguenti responsabilità previste dalla normativa vigente in materia.

Pertanto, a seguito dell'adozione della presente Policy, l'ASP auspica che l'utilizzo delle risorse informatiche e telematiche aziendali avverrà nell'ambito del generale contesto di diligenza, fedeltà e correttezza che caratterizza il rapporto lavorativo fra l'ASP e i propri dipendenti e/o collaboratori e, quindi, che verranno adottate tutte le cautele e le precauzioni necessarie per evitare le possibili conseguenze dannose che un utilizzo non avveduto dei suddetti strumenti può comportare.

La presente Policy è conforme ai principi stabiliti dal D. Lgs. 08.06.2001, n. 231 ("Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'articolo 11 della legge 29.09.2000, n. 300"), dal D. Lgs. 30.06.2003, n. 196, così come modificato ed integrato dal D. Lgs. 10.08.2018, n. 101 ("Codice in materia di dati personali" o "Codice Privacy"), dal Regolamento UE 2016/679 del Parlamento europeo e del Consiglio del 27.04.2016

© Documento valido ed utilizzabile dal Titolare del trattamento esclusivamente a fini di conformità interna

relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (c.d. "Regolamento generale sul trattamento dei dati personali" o "GDPR"), nonché dai provvedimenti del Garante per la tutela dei dati personali.

Essa sarà regolarmente adeguata ed aggiornata rispetto ai mutamenti normativi ed alle minacce future e, si precisa che, per quanto non previsto nel presente documento, si applicheranno le disposizioni di legge vigenti.

La Policy dell'ASP è suddivisa nei seguenti capitoli:

Nel primo capitolo, vengono indicati i motivi per cui l'ASP ha ritenuto conforme alle proprie politiche aziendali di procedere all'adozione di una Policy sulla sicurezza informatica al fine di sensibilizzare tutti i dipendenti e/o collaboratori della ASP e gli altri soggetti alla stessa cointeressati. Inoltre, vengono illustrate le procedure e le attività di controllo su cui si fonda la Policy stessa specificandone le finalità.

Nel secondo capitolo vengono fissate le modalità di diffusione della Policy e della formazione del personale.

Nel terzo capitolo vengono sancite le regole di utilizzo delle postazioni di lavoro e imposti determinati obblighi ai dipendenti e/o collaboratori.

Nel quarto capitolo vengono indicate le modalità di gestione degli strumenti informatici affidati al dipendente in caso di assenza o per motivi di urgente necessità.

Nel quinto capitolo vengono illustrate le modalità di gestione delle password e stabiliti determinati obblighi comportamentali.

Nel sesto capitolo vengono fornite ai dipendenti e/o collaboratori e/o collaboratori le raccomandazioni sul corretto utilizzo della posta elettronica dell'A.S.P. COLLEGIO MORIGI - DE CESARIS.

Nel settimo capitolo vengono introdotte le modalità di utilizzo della rete internet da parte dei dipendenti e/o collaboratori e/o collaboratori e le relative azioni non consentite.

Nell'ottavo capitolo vengono illustrate le regole da seguire per il corretto utilizzo dei dispositivi mobili aziendali come Tablet e Smartphone.

Nel nono capitolo vengono descritti i sistemi di sicurezza installati sui computer dell'A.S.P. COLLEGIO MORIGI - DE CESARIS che salvaguardano l'accesso ad Internet da parte dei lavoratori.

Nel decimo capitolo vengono illustrati i sistemi di monitoraggio e le modalità di verifica attuate dall'A.S.P. COLLEGIO MORIGI - DE CESARIS con a fronte di eventuali eventi anomali all'interno dei sistemi informatici aziendali, finalizzati unicamente all'accertamento del rispetto delle regole imposte dalla presente Policy.

Nell'undicesimo capitolo vengono indicate le misure di sicurezza adottate al fine di garantire l'accessibilità ai dati personali detenuti e agli strumenti elettronici in caso di danneggiamento.

Nel dodicesimo ed ultimo capitolo vengono stabilite le sanzioni, il relativo sistema disciplinare ed i provvedimenti adottati da ASP in caso di mancata osservanza della Policy.

© Documento valido ed utilizzabile dal Titolare del trattamento esclusivamente a fini di conformità interna

INDICE

© Documento valido ed utilizzabile dal Titolare del trattamento esclusivamente a fini di conformità interna