

# MODELLO ORGANIZZATIVO PER LA PROTEZIONE DEI DATI PERSONALI (MOGP)

edizione 1 del 25 luglio 2018

redatto secondo il GDPR 679/16

ente proprietario del Modello  
CONGREGAZIONE  
DELLE PICCOLE FIGLIE  
DEL SACRO CUORE DI GESÙ

INDIVIDUAZIONE DELLE SEDI A CUI SI APPLICA IL PRESENTE MODELLO PRIVACY	ATTIVITÀ SVOLTA IN CIASCUNA SEDE
Piazzetta S. Stefano, 1 - ASTI	Pensionato per persone autosufficienti
Via Giobert, 64 -ASTI	Convitto
"Pastor Angelicus" – Via P.F. Cittadini, 5 - MILANO	Scuola paritaria primaria e scuola secondaria di 1° grado
"Casa Sacro Cuore" – Via Lago, 89 – Besozzo (VA)	Scuola paritaria dell'infanzia e scuola primaria
"Margherita Remotti" - Via Mons. A. Boccio, 54 – Nola (NA)	Scuola paritaria dell'infanzia e scuola primaria
"Casa Gesù Bambino" – Via sul Monte, 5 – Cerro di Laveno (VA)	Casa per Ferie
Casamadre – Via Mons. A. Boccio, 2 – Sale (AL)	Coordinamento attività della Congregazione

## 1. Principi Generali

La Congregazione delle Piccole Figlie del Sacro Cuore di Gesù adotta un Modello Organizzativo Privacy allo scopo di applicare in modo corretto il GDPR, tenendo conto delle caratteristiche specifiche della propria attività e della tipologia di dati personali che tratta. Trattandosi di un Modello Organizzativo, il presente documento si basa sui seguenti elementi:

- attribuzione di ruoli e responsabilità all'interno dell'ente per la protezione dei dati personali;
- svolgimento da parte dell'OdV (Organismo di Vigilanza secondo il D. Lgs. 231/01) con compiti di consulenza, assistenza e sorveglianza rispetto all'applicazione del GDPR, in sostituzione del DPO che la Congregazione non ha ritenuto necessario nominare, non rientrando nella casistica degli enti obbligati secondo il GDPR;
- definizione di una politica per la protezione dei dati personali;

- mappatura di tutti i dati personali trattati dall'ente con individuazione dei trattamenti a rischio e delle conseguenti azioni dirette ad assicurare il controllo del rischio;
- contrattualizzazione degli impegni per la Privacy che devono assumere i soggetti terzi che trattano dati per conto dell'ente;
- approvazione di un regolamento aziendale per la Privacy che costituisce attuazione del codice etico dell'ente;
- predisposizione dell'informativa agli interessati chiara, completa e di semplice comprensione.

## **2. Riferimenti normativi**

Il presente Modello Organizzativo Privacy (a seguire solo **MOGP**) è stato definito in conformità con il Regolamento UE 2016/679 relativo alla protezione dei dati personali (a seguire solo **GDPR**), anche alla luce delle Linee Guida, dei Provvedimenti e delle altre indicazioni pubblicate sul sito dell'Autorità Garante per la Protezione dei Dati Personali (a seguire solo **Garante**).

Nella definizione del Modello si è altresì tenuto conto dell'impostazione generale di tutti i sistemi di gestione contenuta nella Norma Uni En Iso 9001:2015.

## **3. Illustrazione dei concetti chiave contenuti nel MOGP**

Il MOGP utilizza la terminologia per la Privacy contenuta nell'articolo 24 GDPR, con particolare riferimento ai seguenti concetti, qui riportati in forma ridotta e semplificata per favorirne la comprensione a tutti gli operatori dell'ente:

- **dato personale:** qualsiasi informazione riguardante una persona fisica identificata o identificabile (interessato);
- **trattamento:** qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
- **profilazione:** qualsiasi forma di Trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;
- **pseudonimizzazione:** il Trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;

- **archivio:** qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;
- **titolare del Trattamento:** la persona fisica o giuridica che, singolarmente o insieme ad altri, determina le finalità e i mezzi del Trattamento di dati personali;
- **responsabile del Trattamento:** la persona fisica o giuridica che tratta dati personali per conto del Titolare del Trattamento;
- **consenso dell'interessato:** qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di Trattamento;
- **violazione dei dati personali (data breach):** la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;
- **dati biometrici:** i dati personali ottenuti da un Trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;
- **dati relativi alla salute:** i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;
- **impresa:** la persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le società di persone o le associazioni che esercitano regolarmente un'attività economica;

#### **4. Politica dell'ente per la Privacy**

La Congregazione delle Piccole Figlie del Sacro Cuore di Gesù pone alla base del proprio sistema di gestione per la Privacy la presente Politica per la Protezione dei Dati Personali, che costituisce la fondamentale assunzione d'impegno da parte dell'ente rispetto a tutti gli stakeholders del proprio sistema Privacy (utenti, lavoratori, fornitori, Garante...).

La Congregazione s'impegna di fronte a tutte le parti interessate ad osservare i seguenti comportamenti in materia di protezione dei dati personali:

- I. individuare al proprio interno le figure coinvolte nel Trattamento dei dati e fornire loro adeguata formazione, supporto tecnico e sufficienti risorse;
- II. attribuire all'OdV il compito di assistere l'ente nell'applicazione della normativa sulla Privacy;
- III. trattare tutti i dati personali in modo lecito, corretto e trasparente nei confronti dell'interessato;
- IV. trattare i dati personali solo in presenza di una delle seguenti condizioni di liceità previste dal GDPR:
  - a) l'interessato ha espresso il consenso al Trattamento dei propri dati personali per una o più specifiche finalità;

- b) il Trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte;
  - c) il Trattamento è necessario per adempiere un obbligo legale al quale è soggetto il Titolare del Trattamento;
  - d) il Trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;
  - e) 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;
  - f) 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 che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.
- V. raccogliere dati solo per finalità determinate, esplicite e legittime;
  - VI. trattare i dati in possesso dell'ente in modo compatibile con le finalità per le quali sono raccolti, senza alcun Trattamento eccedente rispetto ad esse;
  - VII. astenersi di regola dal trattare senza il consenso esplicito dell'interessato i suoi dati sensibili, vale a dire personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona;
  - VIII. applicare il principio della minimizzazione dei dati, in base al quale il Trattamento dei dati viene limitato allo stretto indispensabile in relazione alle finalità per le quali i dati sono raccolti;
  - IX. raccogliere i dati in modo esatto, correggere tempestivamente i dati non esatti ed aggiornarli ogni volta che sia necessario;
  - X. conservare i dati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati;
  - XI. trattare i dati personali secondo i principi di integrità e riservatezza, quindi in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali;
  - XII. svolgere periodicamente audit interni sul sistema Privacy, attraverso l'OdV o altri soggetti competenti ed indipendenti;
  - XIII. informare in modo completo e comprensibile gli interessati dei trattamenti effettuati;
  - XIV. predisporre, sotto la vigilanza dell'OdV, un Registro di tutti i trattamenti effettuati, comprensivo della valutazione del rischio per ciascun Trattamento;
  - XV. adottare adeguati provvedimenti disciplinari nei confronti degli addetti dell'ente che non osservano le disposizioni del GDPR e le norme aziendali sulla Privacy;
  - XVI. garantire ad ogni interessato i diritti di accesso, rettifica e cancellazione dei dati che lo riguardano.

## **5. Organigramma per la Privacy**

La Congregazione delle Piccole Figlie del Sacro Cuore di Gesù attribuisce al proprio interno i seguenti compiti relativamente al Trattamento dei dati personali:

<b>ruolo</b>	<b>caratteristiche</b>	<b>chi ricopre il ruolo nell'ente</b>
Titolare del Trattamento	Soggetto con l'autorità ed i poteri per definire le finalità del Trattamento e decidere le misure tecniche e organizzative	Congregazione, per il tramite della Legale Rappresentante
Responsabile interno del Trattamento	Soggetto che effettua un Trattamento per conto del Titolare definendo, sotto il controllo del Titolare, mezzi e modalità del Trattamento	Coordinatore didattico della scuola e Responsabile delle attività per le altre case
Responsabile esterno del Trattamento	Fornitore esterno dell'Ente che effettua un Trattamento per conto del Titolare definendo, sotto il controllo del Titolare, mezzi e modalità del Trattamento	Consulenti paghe Consulenti informatici
Incaricato del Trattamento	Soggetto che esegue singole operazioni rispetto ai dati personali senza alcuna autonomia decisionale, nel rispetto delle istruzioni di Titolare e responsabile	Tutti gli addetti (dipendenti, suore e collaboratori) che trattano dati conferiti dall'interessato alla Congregazione quale titolare del trattamento

## **6. Principi Generali del GDPR sul Consenso al Trattamento dei dati**

L'articolo 7 del GDPR prevede le seguenti caratteristiche dell'atto di consenso al Trattamento dei dati personali, da parte del soggetto interessato.

1. Qualora il Trattamento sia basato sul consenso, il Titolare del Trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al Trattamento dei propri dati personali.
2. Se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. Nessuna parte di una tale dichiarazione che costituisca una violazione del presente regolamento è vincolante.
3. L'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento. La revoca del consenso non pregiudica la liceità del Trattamento basata sul consenso prima della revoca. Prima di esprimere il proprio consenso, l'interessato è informato di ciò. Il consenso è revocato con la stessa facilità con cui è accordato.

4. Nel valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al Trattamento di dati personali non necessario all'esecuzione di tale contratto.

Rilevante a tale scopo è anche il Considerando 32 del GDPR, in base al quale Il consenso dovrebbe essere espresso mediante un atto positivo inequivocabile con il quale l'interessato manifesta l'intenzione libera, specifica, informata e inequivocabile di accettare il Trattamento dei dati personali che lo riguardano, ad esempio mediante dichiarazione scritta, anche attraverso mezzi elettronici, o orale. Ciò potrebbe comprendere la selezione di un'apposita casella in un sito web, la scelta di impostazioni tecniche per servizi della società dell'informazione o qualsiasi altra dichiarazione o qualsiasi altro comportamento che indichi chiaramente in tale contesto che l'interessato accetta il Trattamento proposto. Non dovrebbe pertanto configurare consenso il silenzio, l'inattività o la preselezione di caselle. Il consenso dovrebbe applicarsi a tutte le attività di Trattamento svolte per la stessa o le stesse finalità. Qualora il Trattamento abbia più finalità, il consenso dovrebbe essere prestato per tutte queste. Se il consenso dell'interessato è richiesto attraverso mezzi elettronici, la richiesta deve essere chiara, concisa e non interferire immotivatamente con il servizio per il quale il consenso è espresso.

L'ente s'impegna pertanto a raccogliere il consenso al Trattamento dei dati personali nel rispetto dei criteri del GDPR sopra riportati ed a tale scopo prevede i Modelli contenuti nei paragrafi successivi del MOGP, che potranno essere adattati e revisionati in base alla tipologia di dati in questione ma che costituiscono comunque una traccia di riferimento improntata al rispetto dei principi del GDPR sulla manifestazione del consenso.

## **7. Formazione ed aggiornamento del personale in materia di Privacy**

Il Titolare del Trattamento, con l'assistenza dell'OdV, organizza la formazione e l'aggiornamento periodico di tutto il personale dell'ente in materia di Privacy.

Per la formazione sulla Privacy sono previsti i seguenti contenuti minimi:

- formazione iniziale di almeno 2 ore al personale apicale e non apicale sul GDPR e sul MOGP adottato dall'ente;
- aggiornamento continuo di almeno 2 ore ogni triennio.

## **8. Principi Generali sul Registro dei Trattamenti**

L'articolo 30 del GDPR prevede che ogni Titolare del Trattamento e, ove applicabile, il suo rappresentante tengono un registro delle attività di Trattamento svolte sotto la propria responsabilità. Tale registro contiene tutte le seguenti informazioni:

- il nome e i dati di contatto del Titolare del Trattamento e, ove applicabile, del contitolare del Trattamento, del rappresentante del Titolare del Trattamento e del responsabile della protezione dei dati;
- le finalità del Trattamento;
- una descrizione delle categorie di interessati e delle categorie di dati personali;
- le categorie di destinatari a cui i dati personali sono stati o saranno comunicati;

- i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- una descrizione generale delle misure di sicurezza tecniche e organizzative adottate dall'ente.

Lo stesso Regolamento prevede che tale obbligo non si applica di regola alle imprese o organizzazioni con meno di 250 dipendenti, ma l'ente reputa comunque opportuno dotarsi, anche su base volontaria, del Registro, quale documento chiave per la gestione del MOGP.

## **9. Modello di Registro dei Trattamenti e successiva Analisi dei Rischi**

L'ente adotta un Registro dei Trattamenti, che sarà implementato ed aggiornato sotto a vigilanza dell'OdV e di tutte le funzioni coinvolte nella gestione della Privacy, sotto forma di tabella, sviluppando una riga per ogni categoria di dati trattati ed inserendo nelle colonne le seguenti informazioni:

- Ambito e Finalità del Trattamento
- Incaricati
- Categorie di interessati
- Categorie di dati personali
- Modalità raccolta dati
- Modalità del Trattamento
- Base di Liceità del Trattamento
- Misure organizzative e di sicurezza attuate
- Comunicazioni all'interno
- Comunicazione all'esterno
- Luogo custodia file
- Luogo custodia cartaceo
- Tempi di conservazione
- Cessazione Trattamento

Tale mappatura costituisce la fase essenziale di applicazione del GDPR, poiché consente di individuare i trattamenti esposti al maggior rischio e, con la supervisione dell'OdV, richiedere l'aggiornamento del Registro sollecitando l'adozione di ulteriori misure organizzative e di sicurezza, qualora quelle già in essere non fossero ritenute sufficienti rispetto ai rischi.

Una volta completato il Registro, infatti, il Titolare del trattamento, insieme al Responsabile di ogni casa, provvederà a definire un'analisi dei rischi e richiedere le conseguenti azioni di miglioramento.

## **10. Comportamenti da adottare in caso di violazione dei dati personali**

L'articolo 33 del GDPR prevede quanto segue:

- In caso di violazione dei dati personali, il Titolare del Trattamento notifica la violazione al Garante senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.

- Il responsabile del Trattamento informa il Titolare del Trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.
- La notifica al Garante deve almeno:
  - descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
  - comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
  - descrivere le probabili conseguenze della violazione dei dati personali;
  - descrivere le misure adottate o di cui si propone l'adozione da parte del Titolare del Trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.
- Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.
- Il Titolare del Trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio.

L'articolo 34, in merito alla comunicazione di una violazione dei dati personali all'interessato, prevede invece quanto segue:

- Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare del Trattamento comunica la violazione all'interessato senza ingiustificato ritardo.
- La comunicazione all'interessato descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni e le misure di cui all'articolo 33.
- Non è richiesta la comunicazione all'interessato di cui al paragrafo 1 se è soddisfatta una delle seguenti condizioni:
  - il Titolare del Trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
  - il Titolare del Trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;
  - detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.
- Nel caso in cui il Titolare del Trattamento non abbia ancora comunicato all'interessato la violazione dei dati personali, l'autorità di controllo può richiedere, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, che vi provveda o può decidere che una delle condizioni sopra individuate sia soddisfatta.



## **11. Check list per la verifica di compliance rispetto alla tutela della Privacy**

Un auditor incaricato dall'OdV effettua periodicamente audit di compliance rispetto alla tutela della Privacy ed all'osservanza del GDPR, delle indicazioni del Garante e delle regole aziendali per la Privacy.

Le check list di audit sono definite volta per volta, sulla base degli elementi che l'auditor intende sottoporre a verifica, anche alla luce delle criticità che si siano eventualmente verificate.

Una possibile traccia per la check list, soprattutto nella fase iniziale di adeguamento al GDPR, è la seguente, ispirata alle misure minime di sicurezza previste dalla legislazione italiana antecedente all'approvazione del GDPR:

È stato predisposto un Regolamento aziendale per l'utilizzo degli strumenti informatici e delle reti aziendali da parte dei lavoratori?

I soggetti (persone fisiche o giuridiche) preposti da Titolare al Trattamento di dati personali sono stati designati per iscritto Responsabili del Trattamento?

Sono state fornite precise istruzioni per il Trattamento?

Sono stati nominati per iscritto l'amministratore di sistema e il custode delle credenziali?

Sono stati nominati per iscritto i Responsabili esterni del Trattamento (es. prestazione servizi in *outsourcing*)?

È stato predisposto un accordo con eventuali contitolari?

Viene aggiornata la lista di Incaricati, Responsabili e Amministratori di sistema? Ogni quanto? Qual è la data dell'ultimo aggiornamento?

Sono verificati periodicamente i profili e i livelli di autorizzazione di Incaricati, Responsabili e Amministratori di sistema?

Sono state adottate le misure di sicurezza obbligatorie richieste dalla normativa per trattamenti con strumenti elettronici?

Sono state adottate le misure di sicurezza obbligatorie richieste dalla normativa per trattamenti senza l'ausilio di strumenti elettronici?

È stata predisposta e viene aggiornata una lista delle misure di sicurezza adottate?

### **INFORMATIVA E CONSENSO**

Sono state mai effettuate delle notificazioni del Trattamento (es. per profilazione, geolocalizzazione)?

È stato acquisito (e documentato per iscritto) il consenso degli interessati a cui si riferiscono i dati personali oggetto di Trattamento?

È stato acquisito il consenso prestato in forma scritta degli interessati a cui si riferiscono i dati sensibili eventualmente oggetto di Trattamento?

È stato acquisito (e documentato per iscritto) il consenso degli interessati a cui si riferiscono i dati personali oggetto di Trattamento per finalità di marketing?

È stato acquisito (e documentato per iscritto) il consenso degli interessati a cui si riferiscono i dati personali oggetto di Trattamento per finalità di profilazione?

È stato acquisito (e documentato per iscritto) il consenso degli interessati a cui si riferiscono i dati personali oggetto di Trattamento per le finalità puntualmente indicate nell'informativa?

## **COMPLIANCE SISTEMI INFORMATICI**

Le credenziali sono costituite da:  
codice e parola chiave?

Dispositivo di autenticazione?  
Caratteristica biometrica?

Ad ogni incaricato sono assegnate o  
associate individualmente una o più  
credenziali?

Sono state fornite istruzioni per  
assicurare la segretezza delle  
credenziali?

La password di tutti gli operatori: è  
composta da almeno 8 caratteri?  
Contiene riferimenti riconducibili  
all'incaricato? Viene modificata  
dall'incaricato al primo utilizzo e  
almeno ogni sei mesi nel caso di  
Trattamento di dati personali comuni  
o tre mesi nel caso di Trattamento di  
dati sensibili o giudiziari?

Il codice di autenticazione (login) non  
è assegnato ad altri incaricati,  
neppure in tempi diversi?

Le credenziali di autenticazione non  
utilizzate da almeno sei mesi sono  
disattivate salvo quelle  
preventivamente autorizzate per soli  
scopi di gestione tecnica?

Le credenziali sono disattivate anche  
in caso di perdita del ruolo da parte  
del soggetto a cui erano state  
assegnate?

Sono state date istruzioni per non  
lasciare incustodito e accessibile il pc  
o il device?

Si adottano modalità con le quali il  
Titolare può assicurare la  
disponibilità in caso di assenza o  
impedimento dell'incaricato?

Vengono custodite le copie delle credenziali di autenticazione?

Quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso è utilizzato un sistema di autorizzazione tramite lettere di nomina differenziate?

Vengono individuati e configurati i profili tramite lettere di nomina anteriormente all'inizio del Trattamento?

Periodicamente e comunque almeno annualmente è verificata la sussistenza delle condizioni (verifica della coerenza delle lettere con le mansioni svolte)?

Sono stati nominati per iscritto tutti gli incaricati?

La lista degli incaricati è stata redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione?

I dati personali risultano protetti contro il rischio di intrusione e dell'azione di programmi mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale?

Gli aggiornamenti periodici dei programmi per prevenire la vulnerabilità di strumenti e per correggere difetti sono stati effettuati nel corso dell'anno (semestralmente per dati sensibili o giudiziari)?

Sono state conferite istruzioni organizzative e tecniche per il salvataggio dei dati con frequenza almeno settimanale?

Sono state implementate e verificate le procedure di back up?

Sono presenti strumenti e procedure per verificare la compliance alle istruzioni presenti nell'Information Security Policy e al Regolamento

## **GESTIONE TRATTAMENTO DATI PERSONALI**

Che tipo di personale viene impiegato per la gestione e l'amministrazione della sicurezza del sistema informativo? Solo personale interno? Personale misto?

La gestione sicurezza è affidata in outsourcing?

Per quali finalità sono trattati i dati personali?

Dove sono conservati i dati personali trattati e per quanto tempo?

Esistono policy sulle tempistiche di conservazione ed eventualmente di cancellazione dei dati personali trattati da questo reparto?

I dati personali trattati sono archiviati/trasmessi/comunicati anche all'esterno dell'organizzazione aziendale? A quali soggetti? Fornitori esterni? Consulenti? Provider? Altri?

Nel caso di acquisizione di prodotti o servizi IT, vengono considerate certificazioni di sicurezza?

Se si utilizzano UserID e password come sistema di autenticazione, sono state definite regole per la gestione delle password?

Ci si assicura che gli utenti siano a conoscenza di tali regole e delle altre

regole aziendali per l'uso delle risorse informatiche e telematiche?

Se si utilizzano UserID e password come sistema di autenticazione, è prevista la scadenza automatica di account/password?

Se si utilizzano UserID e password come sistema di autenticazione, esiste un controllo preventivo della scelta della password?

Con quale frequenza viene verificata la presenza di aggiornamenti dei server?

Si effettua il monitoraggio della sicurezza del sito web?

Si è svolto secondo le modalità e i tempi previsti nel DPS o altro manuale/procedura?

Le credenziali di accesso alla rete sono correttamente utilizzate, protette e aggiornate?

Sono state sviluppate procedure di ripristino e reporting in caso di accessi abusivi/data breach

## **RISORSE UMANE**

Sono stati predisposti strumenti di identificazione/autenticazione per l'accesso fisico o informatico ad alcune aree aziendali o del sistema informatico?

Se sì, come sono disciplinati?

Quali sono le forme di identificazione/autenticazione previste? Badge??

Forme di riconoscimento biometrico?

Come sono strutturati e gestiti i data base relativi ai dati personali e sensibili dei dipendenti?

Esiste una policy che disciplini i criteri e le modalità di accesso ai dati personali e sensibili dei dipendenti?

Sono stati predisposti diversi livelli di accesso e di protezione ai dati sensibili dei dipendenti? Come sono disciplinati?

Quali criteri/sistemi di autenticazione per l'accesso alla rete interna vengono utilizzati?

Quali criteri/sistemi di autenticazione per determinate categorie di dati sensibili riguardanti il personale vengono utilizzati?

Ci si assicura che gli utenti siano a conoscenza di tali regole e delle altre regole aziendali per l'uso delle risorse informatiche e telematiche?

Viene effettuata la conservazione a norma di documenti contenenti dati personali?

## **REPARTO LEGAL-AMM.VO-CONTABILE**

Quali criteri/sistemi di autenticazione per l'accesso alla rete interna vengono utilizzati?

Quali criteri/sistemi di autenticazione per determinate categorie di dati sensibili riguardanti il personale o i clienti vengono utilizzati?

Se si utilizzano UserID e password come sistema di autenticazione, sono state definite regole per la gestione delle password?

Ci si assicura che gli utenti siano a conoscenza di tali regole e delle altre regole aziendali per l'uso delle risorse informatiche e telematiche?

Sono dati in dotazione ai lavoratori device aziendali? Se sì, con quali finalità? Sono raccolti dati relativi all'attività lavorativa?

Viene effettuata la conservazione a norma di documenti contenenti dati personali?

### **12. Attuazione delle indicazioni del Garante per la Privacy nelle scuole**

Il MOGP relativo alle attività scolastiche ed educative tiene conto delle indicazioni specifiche fornite dall'Autorità Garante, che si riassumono nei punti seguenti, ritenuti applicabili anche alla Congregazione e vincolanti per tutto il personale che opera nell'ente:

- I. tutte le scuole hanno l'obbligo di far conoscere agli interessati (studenti, famiglie, professori...) come vengono trattati i loro dati personali, rendendo noto, attraverso un'adeguata informativa, quali dati raccolgono, come li utilizzano ed a quale fine;
- II. nelle scuole paritarie e nei CfP accreditati la base legale per il Trattamento è il consenso dell'interessato o di chi esercita la tutela per gli alunni minorenni, che tuttavia non va richiesto per i trattamenti che la scuola adotta per adempiere agli obblighi di legge o per adempiere al contratto d'iscrizione. Il Garante specifica quindi che il consenso va acquisito per le attività non strettamente connesse a quelle didattiche o non già previste dall'ordinamento scolastico;



- III. le scuole, nel raccogliere le iscrizioni, possono adattare i relativi moduli per raccogliere i dati necessari alla realizzazione della propria offerta formativa, ma non possono includere la richiesta di informazioni personali eccedenti e non rilevanti per il perseguimento di tali finalità, come ad esempio lo stato di salute dei nonni.
- IV. È necessario però che, nel pubblicare i voti degli scrutini e degli esami nei tabelloni, l'istituto scolastico eviti di fornire, anche indirettamente, informazioni sulle condizioni di salute degli studenti, o altri dati personali non pertinenti. Il riferimento alle "prove differenziate" sostenute dagli studenti portatori di handicap o con disturbi specifici di apprendimento (DSA), ad esempio, non va inserito nei tabelloni, ma deve essere indicato solamente nell'attestazione da rilasciare allo studente;
- V. Il diritto-dovere di informare le famiglie sull'attività e sugli avvenimenti della vita scolastica deve essere sempre bilanciato con l'esigenza di tutelare la personalità dei minori. È quindi necessario evitare di inserire, nelle circolari e nelle comunicazioni scolastiche non rivolte a specifici destinatari, dati personali che rendano identificabili, ad esempio, gli alunni coinvolti in casi di bullismo o in altre vicende particolarmente delicate;
- VI. Le istituzioni scolastiche devono prestare particolare attenzione a non diffondere, anche per mero errore materiale, dati idonei a rivelare lo stato di salute degli studenti, così da non incorrere in sanzioni amministrative o penali. Non è consentito, ad esempio, pubblicare on line una circolare contenente i nomi degli studenti portatori di handicap. Occorre fare attenzione anche a chi ha accesso ai nominativi degli allievi con disturbi specifici dell'apprendimento (DSA), limitandone la conoscenza ai soli soggetti legittimati previsti dalla normativa, ad esempio i professori che devono predisporre il piano didattico personalizzato;
- VII. Su esplicita richiesta degli studenti interessati, le scuole secondarie possono comunicare o diffondere, anche a privati e per via telematica, i dati relativi ai loro risultati scolastici e altri dati personali (esclusi quelli sensibili e giudiziari) utili ad agevolare l'orientamento, la formazione e l'inserimento professionale anche all'estero. Prima di adempiere alla richiesta, gli istituti scolastici devono comunque provvedere a informare gli studenti su quali dati saranno utilizzati per tali finalità.
- VIII. L'utilizzo di telefoni cellulari, di apparecchi per la registrazione di suoni e immagini è in genere consentito, ma esclusivamente per fini personali, e sempre nel rispetto dei diritti e delle libertà fondamentali delle persone coinvolte (siano essi studenti o professori) in particolare della loro immagine e dignità. Le istituzioni scolastiche hanno, comunque, la possibilità di regolare o di inibire l'utilizzo di registratori, smartphone, tablet e altri dispositivi elettronici all'interno delle aule o nelle scuole stesse. Gli studenti e gli altri membri della comunità scolastica, in ogni caso, non possono diffondere o comunicare sistematicamente i dati di altre persone (ad esempio pubblicandoli su Internet) senza averle prima informate adeguatamente e averne ottenuto l'esplicito consenso. Si deve quindi prestare particolare attenzione prima di caricare immagini e video su blog o social network, oppure di diffonderle attraverso mms o sistemi di messaggistica istantanea. Succede spesso, tra l'altro, che una fotografia inviata a un amico o a un familiare venga poi inoltrata ad altri destinatari, generando involontariamente una comunicazione a catena dei dati personali raccolti. Tale pratica può dar luogo a gravi violazioni del diritto alla riservatezza delle persone riprese, e fare incorrere in sanzioni disciplinari, pecuniarie e in eventuali reati;

- IX. È possibile installare un sistema di videosorveglianza negli istituti scolastici quando risulti indispensabile per tutelare l'edificio e i beni scolastici, circoscrivendo le riprese alle sole aree interessate, come ad esempio quelle soggette a furti e atti vandalici. Le telecamere che inquadrano l'interno degli istituti possono essere attivate solo negli orari di chiusura, quindi non in coincidenza con lo svolgimento di attività scolastiche ed extrascolastiche. Le aree perimetrali esterne, al pari di ogni altro edificio pubblico o privato, possono invece essere oggetto di ripresa, per finalità di sicurezza, anche durante l'orario di apertura dell'istituto scolastico. In questo caso, l'angolo visuale deve essere delimitato in modo da non inquadrare luoghi non strettamente pertinenti l'edificio. La presenza di telecamere deve sempre essere segnalata da appositi cartelli (vedi i modelli di informativa semplificata predisposti dal Garante e reperibili sul sito [www.garanteprivacy.it](http://www.garanteprivacy.it)), visibili anche di notte qualora il sistema di videosorveglianza sia attivo in tale orario;
- X. La raccolta di informazioni personali, spesso anche sensibili, per attività di ricerca effettuate da soggetti legittimati attraverso questionari è consentita soltanto se i ragazzi, o i genitori nel caso di minori, sono stati preventivamente informati sulle modalità di trattamento e conservazione dei dati raccolti e sulle misure di sicurezza adottate. Studenti e genitori devono comunque essere lasciati liberi di non aderire all'iniziativa;
- XI. Non è possibile utilizzare i dati presenti nell'albo - anche on line - degli istituti scolastici per inviare materiale pubblicitario a casa degli studenti. La conoscibilità a chiunque degli esiti scolastici (ad esempio attraverso il tabellone affisso nella scuola) o di altri dati personali degli studenti non autorizza soggetti terzi a utilizzare tali dati per finalità non previste come, ad esempio, il marketing e la promozione commerciale.