CONVENZIONE CON L'ISTITUTO DELLE AUSILIARIE DIOCESANE PER LE ATTIVITA' DI ASSISTENZA RELIGIOSA SVOLTE PRESSO LA FONDAZIONE IRCCS CA' GRANDA OSPEDALE MAGGIORE POLICLINICO DI MILANO

TRA

La **Fondazione IRCCS Ca' Granda Ospedale Maggiore Policlinico**, con sede in Milano, via Francesco Sforza n. 28, codice fiscale n. 04724150968, di seguito denominata Fondazione, nella persona del Direttore Generale (ex art. 3, comma 6, del D.lgs. 502/1992 e dell'art. 12, comma 10 L.R. 30/12/2009, n. 33) Dr. Nicola Vincenzo Orfeo, domiciliato per la carica presso detta sede,

E

l'**Istituto delle Ausiliarie Diocesane**, con sede in Seveso (Milano), via San Francesco d'Assisi n. 1, codice fiscale n. 08096580157, rappresentato dalla Sorella Maggiore Silvia Angela Fornari, domiciliata per la carica presso detta sede,

SI CONVIENE E SI STIPULA QUANTO SEGUE

ART. 1

L'Istituto delle Ausiliarie Diocesane, come sopra rappresentato, mette a disposizione della Fondazione per le attività di assistenza religiosa presso le Strutture della Fondazione stessa due Consacrate del predetto Istituto, una sorella a tempo pieno ed una con un impegno part-time.

ART. 2

Le attività oggetto della presente convenzione comportano:

a) l'assistenza spirituale e morale dei degenti, dei loro familiari, del personale e di tutti coloro che a qualsiasi titolo fanno parte della comunità ospedaliera;
b) la distribuzione dell'Eucarestia;
c) il contributo in materia di etica e di umanizzazione nella formazione del personale

in attività di servizio;

d) l'accompagnamento spirituale e umano e la relazione d'aiuto;

e) l'animazione liturgica;

f) la collaborazione alle attività pastorali e culturali promosse dal Rettore Vicario e dal Consiglio Pastorale locale.

ART. 3

Le Parti stabiliscono che le Consacrate, adibite all'assistenza religiosa, prevista nella convenzione all'uopo stipulata con l'Ordinario Diocesano della Arcidiocesi di Milano, ed anche in considerazione dell'interesse superiore del servizio reso, collaborano col Rettore Vicario della Parrocchia Ospedaliera mentre resta in capo al Responsabile diretto dell'Istituto di appartenenza la responsabilità gerarchica.

ART. 4

La Sorella Maggiore dell'Istituto ha la facoltà di sostituire le Consacrate quando lo crederà opportuno per le esigenze dell'Istituto o delle Consacrate medesime, con un periodo di almeno un mese di preavviso scritto da comunicarsi all'Ordinario Diocesano ed alla Fondazione.

ART. 5

La Fondazione ha la facoltà di richiedere, per motivi di comprovata gravità, da comunicarsi in via riservata all'Ordinario Diocesano ed alla Sorella Maggiore dell'Istituto, l'avvicendamento o la sostituzione della Consacrata che ritenesse non atta all'assolvimento del ruolo affidato.

ART. 6

Le Consacrate in servizio risiederanno presso la "Casa San Giuseppe" sita all'interna della Fondazione ed affidata da quest'ultima alla Parrocchia Ospedaliera.

ART. 7

Le Parti concordano che, per le attività suesposte, la Fondazione riconosce all'Istituto un compenso annuo complessivo di € 37.800,00, da corrispondere con cadenza mensile.

Tale compenso sarà sospeso nell'ipotesi di cessazione delle Consacrate.

Le Parti concordano, altresì, che le Consacrate hanno diritto di consumare i pasti (prima colazione, pranzo e cena) forniti dalla Fondazione, con oneri e agevolazioni corrispondenti a quelli riconosciuti ai dipendenti della Fondazione medesima.

ART. 8

L'Istituto invierà alla Fondazione, e precisamente alla SC Economico Finanziaria, la ricevuta di avvenuto pagamento.

ART. 9

La copertura assicurativa per la responsabilità civile verso terzi e la garanzia per il rischio infortuni sono a carico della Fondazione, nell'ambito delle corrispondenti polizze.

Alle Consacrate sarà fornito dalla SC Gestione e Sviluppo Risorse Umane della Fondazione un badge per la rilevazione della presenza ai soli fini assicurativi.

ART. 10

Le Parti convengono che per l'esecuzione della convenzione la controparte, nella persona del legale rappresentante pro tempore, è nominato "Responsabile esterno del Trattamento".

Le Parti convengono che il Responsabile è in possesso di adeguate competenze tecniche e know-how circa gli scopi e le modalità di trattamento dei dati personali, delle misure di sicurezza da adottare al fine di garantire la riservatezza, la completezza e l'integrità dei dati personali trattati, nonché circa le norme che disciplinano

la protezione dei dati personali.

Le modalità e le istruzioni per il trattamento dei dati personali impartite dal Titolare al Responsabile costituiscono parte integrante della presente Convenzione (Allegato 1).

Resta inteso che il Titolare ha facoltà di modificare, sostituire o aggiungere istruzioni di trattamento per tutta la durata del trattamento dei dati personali.

Le istruzioni saranno sempre documentate e rese per iscritto, anche tramite supporto elettronico.

Laddove le esigenze contingenti richiedano forma diversa, le istruzioni trasmesse verbalmente o telefonicamente saranno oggetto di formalizzazione scritta non appena possibile.

Qualora le istruzioni fornite siano, a parere del Responsabile, in contrasto con il GDPR o altre disposizioni nazionali ed europee in materia di protezione dei dati personali, il Responsabile dovrà immediatamente informare il Titolare.

Il Responsabile si impegna ad uniformarsi alle disposizioni del GDPR, nonché ad ogni altra disposizione normativa in materia di trattamento dei dati personali attualmente in vigore e/o che venga a modificare, integrare o sostituire l'attuale disciplina.

Nello svolgimento delle attività di trattamento oggetto, il Responsabile tratta i dati personali nella misura funzionale alla prestazione delle attività oggetto della Convenzione e adotta tutte le misure opportune ai sensi dell'art. 32 GDPR.

Il Responsabile garantisce che il personale da esso impiegato è vincolato alla confidenzialità e che lo stesso è formalmente autorizzato al trattamento dei dati personali necessari per l'esecuzione delle attività di cui alla Convenzione e puntualmente istruito sulle modalità.

Salva l'eventuale nomina di Sub-responsabili, il Responsabile si impegna a non

comunicare a terzi né a diffondere per qualsiasi ragione i dati personali senza l'autorizzazione del Titolare, a meno che tale comunicazione non sia necessaria per adempiere obblighi di legge o per ottemperare a un ordine dell'autorità. In tali ipotesi, il Responsabile avviserà tempestivamente per iscritto il Titolare prima di ottemperare a qualsiasi richiesta di comunicazione, salvo che al Responsabile sia proibito da disposizioni normative vigenti.

Il Responsabile mette a disposizione del Titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui all'art. 28 GDPR, anche tramite ispezioni realizzate dal Titolare o da altro soggetto da questi incaricato. A tale scopo il Responsabile riconosce al Titolare, e agli incaricati dal medesimo, il diritto di accedere a locali di pertinenza del Responsabile, supportato e accompagnato dal personale indicato dal Responsabile, ove hanno svolgimento le operazioni di trattamento. Tali ispezioni potranno aver luogo a seguito di comunicazione da parte del Titolare da inviare con un preavviso di almeno cinque giorni lavorativi.

Il Responsabile si impegna collaborare con il Titolare nel rispondere alle richieste dell'Autorità competente.

Il Responsabile si obbliga, altresì, a prestare assistenza al Titolare, nel garantire il rispetto degli obblighi previsti dagli artt. 33 (Notifica di una violazione dei dati personali all'Autorità di controllo), 34 (Comunicazione di una violazione dei dati personali all'interessato) e 35 (Valutazione di impatto sulla protezione dei dati – al riguardo, si rimanda alla sezione 2 al presente accordo) GDPR, tenendo conto della natura del trattamento e delle informazioni di cui ha la disponibilità.

Il Responsabile si impegna a prestare la propria collaborazione per agevolare i Titolari del Trattamento nel garantire il soddisfacimento dei diritti riconosciuti agli interessati dagli artt. 15 – 22 GDPR.

Il Responsabile mette a disposizione del Titolare l'estratto del Registro dei trattamenti ex art. 30 GDPR relativo ai trattamenti eseguiti su sua istruzione.

È fatto divieto al Responsabile di utilizzare, consultare, accedere o porre in essere qualsiasi altro trattamento dei dati personali di cui viene a conoscenza per finalità ulteriori e diverse rispetto a quelle relative al rapporto contrattuale con il Titolare.

Per i trattamenti concernenti dati personali che esulano dall'ambito della presente Convenzione, Titolare e Responsabile danno atto e convengono che ognuna agisce in qualità di autonomo Titolare e sotto la propria distinta responsabilità.

Il Responsabile dichiara di avere una struttura ed una organizzazione adeguata all'esecuzione dell'incarico di trattamento dei dati personali correlato alla presente Convenzione e si impegna ad adeguarla ovvero a mantenerla adeguata alle necessità dell'incarico stesso, garantendo il pieno rispetto (con riguardo ai propri dipendenti ed ai collaboratori interni ed esterni) delle istruzioni sul trattamento dei dati.

Il Responsabile è autorizzato a nominare ulteriori Responsabili del trattamento dei dati personali per l'esecuzione dei trattamenti oggetto del presente accordo e si impegna, altresì, a comunicare immediatamente al Titolare il nome di eventuali ulteriori fornitori di cui intenda avvalersi nell'espletamento dell'incarico ai fini dell'esercizio del diritto di opposizione, che potrà essere comunicata anche a mezzo di posta elettronica.

Il Titolare si riserva il diritto di verificare i Sub-Responsabili e di esercitare il proprio diritto di opposizione qualora i soggetti designati non appaiano in grado di garantire il rispetto della normativa vigente e degli obblighi assunti dal Responsabile.

Il Responsabile si obbliga altresì ad individuare tali operatori tra i soggetti che presentano garanzie sufficienti per mettere in atto misure tecniche ed organizzative adeguate, in modo tale che il trattamento soddisfi i requisiti del GDPR e venga altresì

garantita la tutela dei diritti dell'interessato.

Il Responsabile si obbliga inoltre a stipulare con tali operatori un accordo scritto atto a garantire un grado di protezione pari a quello proprio delle disposizioni della presente Convenzione, con particolare attenzione al diritto di ispezione e verifica, nonché a verificare il rispetto delle prescrizioni in oggetto ed a fornire al Titolare evidenza delle verifiche condotte, su richiesta, ex art. 28, paragrafo 1, GDPR.

Il Responsabile, anche nell'ambito dei sub-affidamenti, non può trasferire i dati personali oggetto dei trattamenti verso le destinazioni di cui all'articolo 44 GDPR senza l'autorizzazione espressa e preventiva del Titolare. Il Responsabile è tenuto a rivolgere al Titolare la richiesta di autorizzazione al trasferimento dei dati in Paesi Extra-UE fornendo la documentazione attestante la legittimità del trasferimento nel rispetto del GDPR. Il Titolare rilascia l'autorizzazione di cui sopra a suo insindacabile giudizio e comunque previa verifica del rispetto delle condizioni di cui al capo V del GDPR.

Le Parti concordano che, con l'accettazione della presente clausola (che rappresenta l'atto di formalizzazione di cui all'art. 28 GDPR), il Responsabile del Trattamento accetta l'incarico che gli è conferito dal Titolare.

Il Responsabile prende altresì atto che l'incarico di effettuare le operazioni di trattamento è affidato per l'esclusiva ragione che il profilo professionale/societario, in termini di proprietà, risorse umane, organizzative ed attrezzature, è stato ritenuto idoneo a soddisfare i requisiti di esperienza, capacità, affidabilità previsti dalla vigente normativa. Qualsiasi mutamento di tali requisiti, che possa sollevare incertezze sul loro mantenimento, dovranno essere preventivamente segnalati al Titolare, che potrà esercitare in piena autonomia e libertà di valutazione il diritto di recesso, senza penali ed eccezioni di sorta.

La presente nomina a Responsabile Esterno del trattamento ha validità per tutta la

durata delle operazioni di trattamento descritte ai paragrafi che precedono e, in ogni caso, per tutta la durata della Convenzione.

Nel caso in cui termini, per qualsiasi ragione, il rapporto contrattuale esistente tra le parti quale presupposto della presente nomina, quest'ultima si intenderà revocata e comunque non produrrà più alcun effetto.

Al momento della cessazione della Convenzione, il Responsabile si impegna a restituire e cancellare tutti i dati trattati per conto del Titolare nello svolgimento delle attività ad esso affidate.

ART. 11

Le Parti con la sottoscrizione della presente convenzione, si impegnano al rispetto delle vigenti norme in materia di prevenzione della corruzione e dei rispettivi codici etici e di comportamento contenuti nel PIAO. In particolare le Parti dichiarano di aver adottato il PIAO con le modalità previste dalla normativa (visibile e consultabile sui rispettivi siti internet), le cui prescrizioni costituiscono parte integrante delle obbligazioni della presente convenzione, assumendo rilevanza anche ai fini di un'eventuale risoluzione del rapporto.

ART. 12

Per quanto non contemplato nel presente atto il rapporto convenzionale è regolato dalle vigenti norme.

Tutti i rapporti di carattere amministrativo, economico e finanziario, connessi con l'espletamento delle prestazioni in argomento, intercorrono esclusivamente tra la Fondazione e l'Istituto delle Ausiliarie Diocesane.

ART. 13

La presente convenzione ha validità dall'1 novembre 2026 e sino al 31 dicembre 2029, salvo disdetta da notificarsi tra le Parti a mezzo lettera Raccomandata R.R.

oppure tramite posta elettronica certificata, con almeno un mese di preavviso.

A decorrere dall'1 novembre 2026 la precedente convenzione stipulata per il triennio 2026/2028, viene revocata e sostituita integralmente dalla presente.

ART. 14

La presente convenzione:

- è soggetta ad imposta di bollo a carico della Fondazione, corrisposta in modo virtuale. Autorizzazione n. 59666/2005 del 07/10/2005. In ottemperanza del D.P.R. 26 ottobre 1972, n. 642 - D.P.R. 30 dicembre 1982, n. 955 e successive modificazioni;
- è soggetta a registrazione solo in caso d'uso, ai sensi dell'art. 5°, 2° comma del D.P.R. 26 aprile 1986 n. 131.

ART. 15

Per qualunque controversia derivante dalla presente scrittura è competente, in via esclusiva, il Foro di Milano.

Letto, confermato e sottoscritto.

Milano, _____

Per Fondazione IRCCS Ca' Granda Ospedale Maggiore Policlinico

Il Direttore Generale (ex art. 3, comma 6, del D.lgs. 502/1992 e dell'art. 12, comma 10 L.R. 30/12/2009, n. 33) **NICOLA VINCENZO ORFEO** _____

Per Istituto Ausiliarie Diocesane

La Sorella Maggiore **SILVIA ANGELA FORNARI** Silvia Angela Fornari

ISTITUTO AUSILIARIE DIOCESANE
Via S. Francesco 1-A SEVESO

Allegato 1

SEZIONE 1

ELENCO DEI TRATTAMENTI DI DATI PERSONALI DI TITOLARITÀ DI **FONDAZIONE IRCCS CA' GRANDA OSPEDALE MAGGIORE POLICLINICO DI MILANO** CHE SONO IN CARICO **ALL'ISTITUTO DELLE AUSILIARIE DIOCESANE** DESIGNATE RESPONSABILE DEL TRATTAMENTO DATI.

Nome Trattamento	Descrizione	Tipologia di dati trattati	Modalità di trattamento	Principali trattamenti
Raccolta ed utilizzo	a) l'assistenza spirituale e morale dei degenti, dei loro familiari, del personale e di tutti coloro che a qualsiasi titolo fanno parte della comunità ospedaliera; b) la distribuzione dell'Eucarestia; c) il contributo in materia di etica e di umanizzazione nella formazione del personale in attività di servizio; d) l'accompagnamento spirituale e umano e la relazione d'aiuto; e) l'animazione liturgica; f) la collaborazione alle attività pastorali e culturali promosse dal Rettore Vicario e dal Consiglio Pastorale locale.	personali	Nessun trattamento	Raccolta ed utilizzo senza conservazione

La precedente tabella riporta integralmente i trattamenti di dati personali legati alle attività oggetto della presente nomina. Ulteriori ed eventuali trattamenti di dati personali sottoposti al medesimo Responsabile del trattamento, nominato mediante il presente Atto di nomina, saranno oggetto di comunicazione da parte del Titolare del trattamento.

Categorie di interessati
Degenti e loro famigliari

Finalità del trattamento
.....

Durata del trattamento
La durata è definita mediante accordo contrattuale tra le Parti o fino all'espletamento delle attività oggetto della presente nomina.

SEZIONE 2

ISTRUZIONI SUL TRATTAMENTO DEI DATI PERSONALI IMPARTITE DA **FONDAZIONE IRCCS CA' GRANDA OSPEDALE MAGGIORE POLICLINICO DI MILANO** IN QUALITA' DI TITOLARE DEL TRATTAMENTO **ALL'ISTITUTO DELLE AUSILIARIE DIOCESANE** DESIGNATO RESPONSABILE DEI TRATTAMENTI DI CUI AL SUDDETTO ATTO DI NOMINA

***

Il ***Responsabile*** del trattamento è tenuto ad effettuare i trattamenti dei dati nel rispetto di quanto disposto dalla normativa privacy e di ulteriori ed eventuali contenuti specifici dell'atto sottoscritto dalle Parti secondo modalità volte a prevenire violazioni dei diritti, delle libertà fondamentali e della dignità degli Interessati, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.

Il ***Responsabile*** è tenuto a trattare i dati personali nel rispetto dei principi di necessità, proporzionalità, pertinenza e non eccedenza, in modo lecito e secondo correttezza, per scopi legittimi e determinati, assicurando l'esattezza e la completezza dei dati e conservando gli stessi in una forma che consenta l'identificazione dell'Interessato per un periodo non superiore a quello occorrente alle finalità per i quali sono stati raccolti e trattati, e provvedendo, quando necessario, alla loro rettifica e aggiornamento.

Il ***Responsabile*** non tratterà i dati personali oggetto dell'incarico per ulteriori finalità.

Il ***Responsabile*** del trattamento si obbliga a svolgere l'incarico nel rispetto delle istruzioni sul trattamento dei dati personali che vengono fornite, oltre che di tutte le norme di legge in materia applicabili anche ai i propri dipendenti ed ai collaboratori esterni.

Il ***Responsabile*** al fine di agevolare la tempestiva collaborazione con il Titolare del Trattamento dei dati personali nell'esecuzione dell'incarico oggetto del presente accordo, indica nella persona del Privacy Officer o del DPO **dell'Istituto delle Ausiliarie Diocesane** il punto di contatto (PDC) al quale il Titolare potrà fare riferimento per ogni comunicazione necessaria o comunque connessa all'esecuzione degli obblighi contrattuali previsti dal presente accordo.

Il ***Responsabile*** è tenuto ad iniziare eventuali nuovi trattamenti solo in seguito a richiesta da parte del Titolare del trattamento.

I server e le infrastrutture informatiche utilizzate per l'esecuzione dei trattamenti di dati personali da parte del ***Responsabile*** si devono trovare all'interno della Comunità Europea e lo stesso vincolo si applica per i server degli ulteriori Responsabili eventualmente nominati secondo quanto previsto dal paragrafo 5 del presente accordo.

Il Responsabile, anche nell'ambito dei sub-affidamenti, non può trasferire i dati personali oggetto dei trattamenti verso le destinazioni di cui all'articolo 44 GDPR senza l'autorizzazione espressa e preventiva del Titolare. Il Responsabile è tenuto a rivolgere al Titolare la richiesta di autorizzazione al trasferimento dei dati in Paesi Extra-UE fornendo la documentazione attestante la legittimità del trasferimento nel rispetto del GDPR e del presente Atto di nomina.

Il Titolare rilascia l'autorizzazione di cui sopra a suo insindacabile giudizio e comunque previa verifica del rispetto delle condizioni di cui al capo V del GDPR. Laddove vengano stipulati accordi relativi al trasferimento transnazionale di dati personali, come, a titolo esemplificativo, Contratti con clausole standard, Norme vincolanti d'impresa o il trasferimento dei dati avvenga secondo Regole Privacy transnazionali, anche tali documenti e l'identità dei paesi o la descrizione delle circostanze in cui i citati accordi sono applicabili verranno debitamente comunicate al Titolare del trattamento.

Il ***Responsabile*** del Trattamento metterà a disposizione del Titolare anche il contratto o il diverso atto vincolante secondo il Diritto dell'Unione o dello Stato Membro con cui l'ulteriore Responsabile del

trattamento si è obbligato nei confronti **dell'Istituto delle Ausiliarie Diocesane** o è stato comunque individuato.
Il ***Responsabile*** informerà il Titolare in tempo breve e, comunque, non oltre giorni 5, di ogni cambiamento in relazione a quanto sopra. In tali casi, il Titolare avrà il diritto di formulare la propria opposizione o di recedere dal contratto con efficacia immediata.
In caso di revoca della designazione a Responsabile dei trattamenti, o, in ogni caso, dopo il completamento di un trattamento per conto del Titolare, il Responsabile deve, sulla base delle istruzioni impartite da quest'ultimo, restituire o cancellare i dati personali, salvo che il diritto dell'Unione o degli Stati membri, cui è soggetto il Responsabile, prescriva la conservazione dei dati personali.
Il ***Responsabile*** deve assicurare in ogni momento che la sicurezza fisica e logica dei dati oggetto di trattamento sia conforme alle norme vigenti, ai documenti contrattuali ed alle specifiche dei Servizi definiti dal ***Titolare***. Le misure di sicurezza adottate dovranno in ogni situazione uniformarsi allo "standard" di maggiore sicurezza fra le disposizioni di legge e gli elementi contrattuali e/o progettuali.
Il ***Responsabile***, in ogni caso, venuto a conoscenza di una specifica violazione dei dati personali, sarà tenuto a comunicare al ***Titolare***, ai sensi dell'art. 33, par. 2 Reg. UE 2016/679, senza ingiustificato ritardo e comunque entro 24 ore dalla scoperta, tali violazioni, eventualmente intervenute durante la vigenza della presente nomina. In ipotesi di intervenute violazioni dei dati personali, il Responsabile del trattamento collaborerà attivamente con il Titolare del trattamento per la corretta gestione della comunicazione delle violazioni summenzionate.
A tal fine, il Responsabile si impegna a comunicare nel termine più breve dalla scoperta e, comunque, non oltre 24 ore da questa, ogni accesso non autorizzato ai dati personali nonché ogni accesso non autorizzato agli strumenti elettronici impiegati per l'esecuzione del trattamento o, comunque, ogni accesso non autorizzato verificatosi presso le strutture del Responsabile che abbiano causato la perdita, la modifica o la rivelazione non dovuta di dati personali.
Nell'ipotesi di violazione dei dati personali ai sensi dell'art. 33 del Regolamento, il Responsabile si doterà di un registro contenente una descrizione dell'evento, del periodo di estensione dello stesso, delle conseguenze prodotte, del nominativo di colui che lo ha riportato oltre che dei soggetti a cui è stato comunicato, della descrizione delle azioni messe in atto per la risoluzione dell'evento (compresa l'indicazione della persona responsabile e i dati recuperati) nonché contenente l'indicazione che è stata cagionata la perdita, la rivelazione o la alterazione di dati personali.
Il Responsabile si impegna inoltre, nei limiti delle proprie competenze, ad adottare, d'intesa con il Titolare, tempestivamente tutte le azioni di contrasto per il contenimento e la mitigazione degli effetti della violazione e ad assistere il Titolare, se richiesto, nella redazione della notifica della violazione all'Autorità di Controllo competente o nella comunicazione agli Interessati coinvolti, a norma degli artt. 33 e 34 GDPR.
Il **Responsabile** implementerà un sistema di gestione del controllo degli accessi ai sistemi e ai dati personali trattati fornendo al Titolare del trattamento nominato, ove occorre, il controllo della gestione degli accessi, ad esempio attribuendo i diritti da amministratore o la gestione delle utenze d'accesso da terminare.
Nelle ipotesi in cui più di una persona abbia accesso ai dati personali archiviati, ognuna di esse verrà dotata di un'autonoma "username" da utilizzare per l'identificazione, autenticazione e per l'individuazione dei livelli di autorizzazione.
Il Responsabile porrà in essere procedure aziendali per la registrazione degli utenti e per la loro de-registrazione, contenenti precise istruzioni per fronteggiare la compromissione del controllo degli accessi da parte degli utenti o degli altri dati relativi alla registrazione (ad es. a causa della compromissione delle credenziali di accesso dell'utente, come nel caso di mal funzionamento o la compromissione di password dovuta a rivelazione involontaria).

Il Responsabile fornirà ogni opportuna e necessaria informazione al Titolare del trattamento in merito all'uso di sistemi di crittografia per la protezione dei dati personali e provvederà altresì a collaborare con il Titolare, fornendo ove necessario ogni necessaria informazione, nel consentire l'applicazione da parte di questi dello stesso livello di protezione dei dati personali.
Il Titolare impiegherà attrezzature contenenti supporti di memorizzazione assicurandosi che tutti i dati personali e i software precedentemente impiegati siano stati rimossi o sovrascritti in maniera sicura, prima dell'eliminazione o del riutilizzo dei supporti stessi.
Nell'assicurare un approccio coerente ed efficace per la gestione degli incidenti relativi alla sicurezza delle informazioni, il Titolare ed il Responsabile prevederanno controlli periodici volti a prevenire e affrontare in maniera adeguata ed efficace gli incidenti di sicurezza.
Un eventuale incidente nella sicurezza delle informazioni dovrà comportare un processo di valutazione da parte del Responsabile del trattamento, come parte del suo processo di gestione degli incidenti, volto a determinare se una violazione delle informazioni riguardante i dati personali ha avuto luogo. Non ogni evento relativo alla sicurezza delle informazioni avrà questo effetto, ma solo quello che causa un effettivo o significativamente probabile accesso non autorizzato ai dati personali o a una delle infrastrutture del Responsabile con le quali viene effettuato il trattamento o ad una delle strutture che contengono dati personali e potrebbe includere, senza alcuna limitazione, ping o attacchi di rete su firewall o edge server, scan delle porte di comunicazione, tentativi di autenticazione non riusciti, attacchi DOS e sniffing di pacchetti.
Il Responsabile del Trattamento metterà inoltre a disposizione del Titolare ogni strumento informatico necessario o comunque utile a consentire l'accesso, la correzione e/o la cancellazione dei dati.
Il ***Responsabile*** è tenuto, in relazione ai soggetti autorizzati al trattamento che agiscono sotto la sua autorità, ad istruire quest'ultimi al rispetto delle seguenti misure, ove ritenute applicabili al trattamento di specie:

1) individuare per iscritto i soggetti autorizzati al trattamento dei dati personali (persone fisiche o gruppi omogenei);
2) impartire ai soggetti autorizzati al trattamento loro le istruzioni idonee alle attività da svolgere;
3) vigilare sull'operato dei soggetti autorizzati al trattamento all'accesso ai dati personali;
4) prevedere un piano di formazione destinato ai soggetti autorizzati al trattamento;
5) assicurarsi che ad ogni soggetto autorizzato al trattamento sia assegnata una credenziale di autenticazione. Le credenziali di autenticazione consistono in un codice per l'identificazione del soggetto autorizzato al trattamento associato a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo del soggetto autorizzato al trattamento, eventualmente associato a un codice identificativo o a una parola chiave;
6) prescrivere necessarie cautele per assicurare la segretezza della componente riservata della credenziale e/o la diligente custodia del dispositivo in possesso ed uso esclusivo del soggetto autorizzato al trattamento;
7) assicurare che la parola chiave, quando è prevista dal sistema di autenticazione, sia composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non deve contenere riferimenti agevolmente riconducibili al soggetto autorizzato al trattamento e deve essere modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni tre mesi;
8) assicurare che il codice per l'identificazione, laddove utilizzato, non possa essere assegnato ad altri soggetti autorizzati al trattamento, neppure in tempi diversi;
9) assicurare che sia operata la disattivazione delle credenziali di autenticazione del personale in caso venga a cessare la necessità di accesso da parte del soggetto autorizzato al trattamento o intervenga un'inattività per più di sei mesi.

10) le credenziali scadute o comunque disattivate non verranno in alcun modo messe a disposizione di altri soggetti.
11) predisporre le necessarie procedure affinché, in caso di prolungata assenza o impedimento del soggetto autorizzato al trattamento che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema, si possa comunque assicurare la disponibilità di dati o strumenti elettronici. In tal caso la custodia delle copie delle credenziali deve essere organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti autorizzati della loro custodia;
12) prevedere, con criteri restrittivi, profili di autorizzazione di accesso per ogni singolo soggetto autorizzato al trattamento o gruppo omogeneo e configurarli prima dell'inizio dei trattamenti;
13) verificare, ad intervalli almeno annuali, le autorizzazioni in essere;
14) redigere e mantenere aggiornato un elenco con gli estremi identificativi delle persone fisiche che rivestono il ruolo di Amministratori di Sistema e, per ciascuno di essi, la descrizione delle funzioni che gli sono state attribuite nell'ambito delle attività svolte per conto del Titolare e implementare le ulteriori misure di sicurezza, come definito nel Provvedimento dell'Autorità Garante per la Protezione dei dati personali del 27/11/2008 "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratori di sistema" e s.m.i.;
15) installare sugli elaboratori idonei programmi contro il rischio di intrusione e accesso abusivo in accordo ai requisiti di legge da aggiornare comunque periodicamente ed in occasione di ogni versione disponibile dalla casa costruttrice;
16) provvedere, ogni qualvolta vi sia la segnalazione della presenza di vulnerabilità nei programmi utilizzati e la contemporanea disponibilità delle opportune modifiche, all'aggiornamento, entro un congruo periodo di tempo, dei programmi utilizzati, o almeno alla valutazione degli impatti sull'aggiornamento;
17) prevedere l'adozione di copie di back-up e il ripristino dei dati in tempi certi.

Il Responsabile garantisce che le persone coinvolte nel trattamento dei dati personali per conto del Titolare, in particolare i dipendenti del Responsabile ed eventuali ulteriori responsabili e loro dipendenti, tratteranno tali dati personali secondo le istruzioni impartite dal Titolare.
Il Responsabile garantisce che il personale impiegato è vincolato alla confidenzialità e che lo stesso è formalmente autorizzato al trattamento dei dati personali necessari per l'esecuzione delle attività di cui al Contratto e puntualmente istruito sulle modalità di esecuzione di tali attività.

In tema di sicurezza dei dati personali, ai sensi dell'art. 32 del Reg. UE 2016/679, il ***Responsabile*** del trattamento è tenuto a mettere in atto misure tecniche ed organizzative idonee a garantire un livello di sicurezza adeguato al rischio. Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.
Inoltre, per il trattamento di categorie particolari di dati personali (c.d. dati particolari), cioè quelli di cui al art. 9, par. 1 del Reg. UE 2016/679, il ***Responsabile*** deve:

1) prevedere che il riutilizzo dei supporti di memorizzazione sia possibile solamente nel caso in cui tutti i dati personali e i software precedentemente utilizzati siano stati rimossi o sovrascritti in maniera sicura, prima dell'eliminazione o del riutilizzo dei supporti stessi; In questo ambito risulta necessario procedere a:
a) emanare adeguate istruzioni di comportamento a tutti i soggetti autorizzati al trattamento;
b) effettuare una ricognizione completa di tutti i supporti di memoria che possano essere riutilizzabili, sia essi di tipo asportabile che presenti in aree di memoria interne al sistema operativo od in programmi, ove possano trovarsi dati particolari;
c) esaminare tutti i nuovi supporti, sistema operativo e programmi, che vengono inseriti nel sistema di trattamento dei dati, analizzando i possibili rischi ed impartendo specifiche istruzioni ai soggetti autorizzati al trattamento.

2) assicurare che la memorizzazione dei dati particolari su elenchi, registri o banche dati, avvenga in maniera da non permettere la diretta identificazione dell'interessato (anche attraverso processi di pseudonimizzazione), ovvero che la memorizzazione dei dati particolari sia cifrata o in alternativa che vi sia separazione tra i dati particolari e gli altri dati personali che possano permettere l'identificazione dell'interessato;

3) assicurare che il trasferimento dei dati particolari in formato elettronico, avvenga attraverso "canali sicuri" o in maniera cifrata.

In merito al **trattamento dei dati personali con strumenti diversi da quelli elettronici,** il ***Responsabile*** è tenuto a predisporre un archivio per gli atti e i documenti con dati personali individuando per iscritto i soggetti autorizzati al trattamento con i relativi profili di accesso ai dati ed ai documenti.
Devono essere definite le procedure di deposito, custodia, consegna o restituzione e compartimentazione dei dati stessi (ad esempio un registro e degli armadi separati e chiusi).
Il trattamento di dati particolari, dovrà infine prevedere l'utilizzo di appositi contenitori con lucchetti o serrature e definire una procedura di gestione delle chiavi.
È fatto comunque assoluto **divieto**, al ***Responsabile*** designato, della **diffusione** dei dati, della **comunicazione** non autorizzata a terzi e più in generale è fatto **divieto** di effettuare trattamenti non finalizzati all'esecuzione delle attività affidate, salvo a fronte di specifica autorizzazione da parte del ***Titolare***.
Le operazioni di trattamento devono essere gestite dal ***Responsabile*** del trattamento in aderenza alle attività svolte nell'ambito dei progetti assegnati e in considerazione di eventuali e successive modifiche alle operazioni e/o modalità di trattamento apportate dal Titolare.
Il ***Responsabile*** è chiamato ad assicurare, per conto del Titolare del trattamento, l'esercizio dei diritti eventualmente applicabili da parte degli Interessati (Capo III del Regolamento UE 2016/679), nel rispetto dei termini di legge, adottando ogni soluzione organizzativa, logistica, tecnica e procedurale idonea ad assicurare l'osservanza delle disposizioni vigenti in materia di trattamento dei dati personali per l'esercizio degli stessi diritti.
Il ***Responsabile*** è tenuto a mettere a disposizione del ***Titolare*** tutte le informazioni necessarie all'espletamento delle attività di revisione, comprese le ispezioni, richieste dallo stesso Titolare del trattamento o da altro soggetto da esso autorizzato, al fine di rilevare il rispetto degli obblighi previsti dalla normativa privacy.
Il ***Responsabile***, ai sensi dell'art. 30 del Regolamento UE 2016/679, è tenuto a fornire al ***Titolare*** le informazioni necessarie a quest'ultimo per la compilazione del proprio "Registro dei trattamenti". Il Responsabile si impegna – nei limiti previsti dalla normativa in materia di protezione dei dati personali – a

conservare le registrazioni relative al trattamento dei dati personali svolto in qualità di Responsabile per conto del Titolare (art. 30, paragrafo 2, GDPR).
Qualora il ***Titolare*** intenda redigere la Valutazione di impatto prevista dall'art. 35 del Regolamento summenzionato, il ***Responsabile*** sarà tenuto a fornire anche le ulteriori informazioni che si rendessero necessarie alla redazione del documento.
Il ***Responsabile***, qualora in ottemperanza all'obbligo di Legge, fosse tenuto ad individuare all'interno della propria organizzazione la figura del "Responsabile per la protezione dei dati personali", quest'ultimo sarà tenuto a svolgere la propria attività in stretta collaborazione con il ***Titolare***.
Il ***Responsabile*** collaborerà attivamente con l'Autorità Garante per la Protezione dei dati personali e le Autorità Pubbliche, al fine di consentire a queste ultime l'esercizio delle proprie attività istituzionali, quali richieste di informazioni, attività di controllo mediante accessi ed ispezioni, relativamente ai trattamenti oggetto dell'Atto di nomina.

ISTITUTO AUSILIARIE DIOCESANE
Via
S. Francesco 1-A
SEVESO

Fornari Silva Angela