

Nomina Responsabile del trattamento dei dati ai sensi dell'art. 28 del Regolamento Generale UE/ 679/2016 e nomina ad Amministratore di Sistema ai sensi e per gli effetti del Provvedimento a carattere generale dell'Autorità Garante per la Protezione dei Dati Personali del 27 Novembre 2008 e ss.mm.ii.

Premesso che

- **Azienda Socio-Sanitaria Territoriale Fatebenefratelli Sacco**, (di seguito "ASST Fatebenefratelli Sacco"), con sede in Milano, via G.B Grassi, 74, (C.F. e P.I.V.A 09319690963), e **Proges Società Cooperativa Sociale** (di seguito "Proges") con sede in Parma, via Colorno, 63, (C.F. e P.IVA01534890346 per il tramite di un accordo di partenariato, di cui Proges ricopre il ruolo di capofila, sono addivenute ad un'intesa ai fini dell'attuazione del progetto "Adriano siCURA. Rete di supporto e prossimità per la salute in età anziana" (anche il "Progetto") su contributo erogato dalla Fondazione Cariplo nell'ambito del bando "Welfare in Ageing";
- Il Progetto, per quanto qui d'interesse, ha quale scopo la presa in carico di persone anziane con fragilità, al fine di offrire, attraverso la definizione multidisciplinare di un Progetto Operativo d'Intervento personalizzato (anche detto "POI"), attività integrate sociosanitarie e sociali;
- La redazione del POI e la gestione delle attività integrate sociosanitarie e sociali da parte di Proges e dell'ASST Fatebenefratelli Sacco comporta il trattamento di dati personali, come definiti all'art. 4, par. 1, del Regolamento (UE) 2016/679 (di seguito anche solo GDPR);
- Sulla scorta di quanto precede le Parti hanno sottoscritto un accordo di contitolarità, ai sensi dell'art. 26 del GDPR, avente ad oggetto i trattamenti di dati personali gestiti in regime di contitolarità tra le stesse durante il periodo di vigenza del rapporto di partenariato, ossia: (i) definizione di un Progetto Operativo d'Intervento (POI) e gestione delle relative attività integrate socio - sanitarie; (ii) gestione dei dati personali dei componenti dell'équipe multidisciplinare;
- Ai fini dello svolgimento delle attività di cui alla lettera B che precede, il Progetto prevede l'utilizzo di una piattaforma, denominata WE CARE, fornita da Applicca SRL ;
- La piattaforma verrà, come previsto dal Progetto, quindi, utilizzata dai Contitolari per le attività di trattamento dei dati personali oggetto di contitolarità;

per l'effetto di quanto precede e di quanto previsto all'Accordo di Contitolarità citato, i Contitolari

Azienda Socio-Sanitaria Territoriale Fatebenefratelli Sacco, con sede in Milano, via G.B Grassi, 74, (C.F. e P.I.V.A 09319690963), e **Proges Società Cooperativa Sociale** (di seguito "Proges") con sede in Parma, via Colorno, 63, (C.F. e P.IVA 01534890346) in qualità di Contitolari del trattamento dei dati personali attribuiscono il ruolo di **responsabile del trattamento dei dati personali e Amministratore di Sistema a:**

Applicca SRL

con sede in Via Dei Mestieri ,sic in Matera (MT) - P.IVA 01211310774, C.F. 01211310774

L'ambito di attività di trattamento dei dati personali delegato dai contitolari al responsabile del trattamento è il seguente: *fornitura, gestione e manutenzione del sistema WE CARE , adottato nell'ambito del progetto "Adriano siCURA, Rete di supporto e prossimità per la salute in età anziana".*

Trattamento: Progetto "Adriano siCURA, Rete di supporto e prossimità per la salute in età anziana"

Finalità del trattamento: messa a disposizione, manutenzione e gestione del sistema _____, utilizzato nell'ambito del progetto "Adriano siCURA, Rete di supporto e prossimità per la salute in età anziana", ai fini della redazione del POI, della gestione delle attività integrate sociosanitarie e della valutazione multidimensionale e multifattoriale svolta dall'équipe multidisciplinare.

Natura del trattamento

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.

Altro

Tipologia dei dati personali trattati

- Comuni identificativi (nome, cognome, dati anagrafici, recapiti di posta elettronica, recapiti telefonici, residenza, etc.).
- Appartenenti a categorie particolari ai sensi dell'art. 9 del Regolamento e idonei a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.
- Dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza.

Categoria dei soggetti interessati

- personale dipendente e collaboratore;
- cittadini aderenti al progetto e/o pazienti.

Tale incarico viene attribuito ai sensi dell'articolo 28 del Regolamento Generale UE/679/2016 (d'ora in avanti denominato semplicemente "Regolamento") e ai sensi e per gli effetti del Provvedimento a carattere generale dell'Autorità Garante per la Protezione dei Dati Personali del 27 Novembre 2008 e ss.mm.ii. (d'ora in avanti anche Provvedimento). Il presente documento rappresenta l'atto giuridico di formalizzazione delle responsabilità come previsto dal paragrafo 3 del citato articolo 28 e dalle disposizioni contenute nel Provvedimento.

Garanzie generali di sicurezza prestate dal Responsabile (Art. 28.1)

Il Responsabile del trattamento (d'ora in avanti anche "Responsabile") garantisce l'attuazione di misure tecniche ed organizzative tali da soddisfare, nella loro totalità, i requisiti posti dal Regolamento.

Autorizzazione nomina Sub-Responsabili (Art. 28.2 – 28.4)

Ai sensi dell'art.28.2 del Regolamento con la presente si fornisce espressa autorizzazione scritta generale alla individuazione da parte del Responsabile di altri soggetti che svolgano, per conto del Responsabile medesimo, il ruolo di "sub-responsabili". A fronte di tale autorizzazione, si richiede al Responsabile di comunicare alla scrivente l'elenco di tutti gli eventuali soggetti individuati in qualità di sub-responsabili. I contitolari provvederanno a verificare eventuali profili di criticità emergenti dalle comunicazioni ricevute e si riservano la facoltà di limitare e/o revocare l'autorizzazione ivi concessa. Nel caso in cui nel tempo intervengano modifiche, aggiunte o sostituzioni dei sub-responsabili inizialmente comunicati, tali nuove nomine dovranno essere inoltrate ai contitolari, al fine di effettuare le opportune valutazioni (anche in termini oppositivi) relativamente alla protezione dei dati personali.

Si precisa come è obbligo del Responsabile individuare e nominare in forma scritta i propri sub-responsabili; tale atto di nomina/individuazione dovrà riproporre a carico del sub-responsabile i medesimi obblighi posti a carico del responsabile e specificati nel presente documento, in particolare l'atto dovrà individuare le misure tecniche ed organizzative adeguate per garantire che il trattamento soddisfi i requisiti di sicurezza richiesti dal Regolamento.

Si evidenzia come il Responsabile conservi nei confronti dei Contitolari del trattamento ogni responsabilità derivante dall'eventuale inadempimento posto in essere dal sub-responsabile.

Prescrizioni poste a carico del Responsabile (art. 28.3)

Per lo svolgimento delle attività di trattamento dati personali conseguenti al servizio affidato al Responsabile, lo stesso dovrà:

- comunicare preventivamente l'eventuale trasmissione dei dati personali verso paese terzo (non appartenente alla Unione Europea); in tali casistiche i Contitolari si riservano la facoltà di esprimere apposita autorizzazione alla trasmissione a meno che tale trasmissione non sia espressamente richiesta dell'Unione o dal diritto nazionale;
- autorizzare espressamente al trattamento dei dati personali i propri dipendenti/collaboratori/soci/volontari attraverso modalità che garantiscano che tali soggetti siano obbligati al rispetto della riservatezza nei confronti dei dati che si troveranno a trattare in funzione del proprio incarico/ruolo;
- garantire di aver effettuato una analisi dei rischi sui trattamenti oggetto della responsabilità e assistere i Contitolari nella valutazione di impatto ai sensi dell'art. 35 del Regolamento tenendo conto della natura del trattamento e delle informazioni a disposizione del Responsabile; i documenti comprovanti l'analisi del rischio e l'eventuale valutazione di impatto dovranno essere messi a disposizione dei Contitolari su richiesta anche di uno solo tra questi;
- garantire la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; le modalità per garantire tali livelli di sicurezza dovranno essere comunicate a ciascun Contitolare nel caso di esplicita richiesta;
- garantire la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico; le modalità per garantire tali livelli di sicurezza dovranno essere comunicate a ciascun Contitolare nel caso di esplicita richiesta;
- garantire la presenza di una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; le modalità per garantire tali livelli di sicurezza dovranno essere comunicate a ciascun Contitolare nel caso di esplicita richiesta;
- garantire che tutti i soggetti che agiscono sotto l'autorità del Responsabile e che abbiano accesso ai dati non trattino tali dati se non sono stati istruiti in tal senso dal Responsabile stesso;
- garantire il necessario apporto a ciascun contitolare del trattamento qualora nei confronti di questo vengano esercitati i diritti che il Regolamento (al capo III) riconosce agli interessati i quali impattino sui dati personali oggetto della presente nomina;
- garantire la comunicazione ai Contitolari (ai sensi dell'art. 33.2 del Regolamento) di tutti gli eventi di violazione dei dati personali al fine di consentire il rispetto delle attività di notifica all'Autorità di controllo stabilite dall'articolo 33 del regolamento. La comunicazione da parte del Responsabile a ciascun Contitolare dovrà avvenire senza ingiustificato ritardo all'indirizzo PEC istituzionale e dovrà contenere almeno i seguenti punti:
 - 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;
- il nome e i dati di contatto del Data Protection Officer o di altro punto di contatto presso cui ottenere più informazioni;
- descrivere le probabili conseguenze della violazione dei dati personali;
- descrivere le misure adottate da parte del Responsabile per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Il Responsabile sarà tenuto a mantenere presso i propri uffici la documentazione necessaria a descrivere le violazioni dei dati subite.

- cancellare entro e non oltre 6 mesi e/o restituire senza ritardo in caso di richiesta a ciascun Contitolare tutti i dati personali, una volta cessata l'erogazione dei servizi relativi al trattamento, cancellando anche le copie esistenti sui propri database, salvo che il diritto dell'Unione o degli stati membri preveda la conservazione dei dati; qualora al termine del servizio il contitolare non richieda espressamente la restituzione dei dati questi si intenderanno soggetti ad obbligo di cancellazione;
- rendersi disponibile a sottoporsi ad attività di auditing da parte di ciascun Contitolare, o di un delegato di quest'ultimo, qualora questo ne ravvisasse la necessità;
- comunicare ai Contitolari l'adesione ad eventuali codici di condotta di cui all'articolo 40 o ad un meccanismo di certificazione di cui all'articolo 42 del Regolamento;
- attenersi ai criteri di durata del trattamento comunicati dai Contitolari.

Prescrizioni poste a carico del responsabile ai sensi del Provvedimento a carattere generale del 27 Novembre 2008 dell'Autorità Garante per la Protezione dei Dati Personali

Ai sensi del Provvedimento il responsabile è stato individuato dal titolare del trattamento dei dati personali in base ad una scrupolosa valutazione dell'esperienza, della capacità, dell'affidabilità e preparazione e fornisce idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento dei dati personali, con particolare riferimento al profilo relativo alla sicurezza nella custodia e nel trattamento dei dati personali.

Il responsabile ha quindi, il potere e il dovere di compiere tutto quanto si renderà necessario ai fini del rispetto e della corretta applicazione delle vigenti disposizioni in materia di trattamento dei dati personali ivi compreso il profilo relativo alla sicurezza.

Il responsabile garantisce ai Contitolari del trattamento che ciascun incaricato quale Amministratore di Sistema accede alle risorse informatiche con credenziali di autenticazione nominative (*username* e *password*).

Con la sottoscrizione di questa nomina il responsabile si impegna a nominare individualmente ai sensi del Provvedimento a carattere generale del 27 Novembre 2008 dell'Autorità Garante per la Protezione dei Dati Personali pubblicato nella Gazzetta Ufficiale N. 300 del 24 dicembre 2008, così come modificato dal successivo Provvedimento dell'Autorità Garante del 25 giugno 2009 pubblicato nella Gazzetta Ufficiale N. 149 del 30 giugno 2009 - gli incaricati della propria struttura che rivestono il ruolo di Amministratori del Sistema informativo. La designazione quale Amministratore di Sistema deve essere individuale e recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato. Annualmente il responsabile fornisce al titolare del trattamento l'elenco aggiornato nominativo degli Amministratori di Sistema e provvede a verificare l'attività dei soggetti individuati, come indicato dall'Autorità Garante.

Il responsabile adotta sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici effettuati da parte dell'Amministratore di Sistema. Le registrazioni (*access log*) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste.

Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi.

Il responsabile è tenuto a:

- garantire che le risorse vengano utilizzate dagli utenti che ne abbiano effettivamente diritto a seguito di apposita comunicazione in tal senso da ciascun Contitolare del trattamento, utilizzando gli opportuni meccanismi di identificazione e autenticazione allo scopo di incrementare il livello di protezione e sicurezza dei trattamenti di dati personali effettuati con strumenti elettronici;
- essere responsabile della gestione dei sistemi di identificazione ed autenticazione, usando la massima riservatezza e discrezione affinché il processo venga svolto in conformità alle disposizioni di legge, eseguendo controlli periodici sull'efficacia delle misure di sicurezza adottate;
- collaborare con i Contitolari del trattamento dei dati alla definizione di idonee regole in ambito di

sicurezza del trattamento dei dati afferente ai sistemi oggetto della presente nomina;

- sovrintendere all'operato dei soggetti terzi idoneamente designati, qualora sia necessario, interni o esterni alla organizzazione di ciascun Contitolare, in caso di interventi tecnici che abbiano impatto sul sistema informativo di ciascun Contitolare e sulla sicurezza del trattamento di dati;
- suggerire, curare e sovrintendere l'adozione e l'aggiornamento delle più ampie misure di sicurezza volte a far sì che i dati personali oggetto di trattamento siano custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;
- aggiornare periodicamente, con frequenza adeguata, i programmi volti a prevenire la vulnerabilità degli strumenti elettronici e a correggerne i difetti o assicurarsi che ciò venga effettuato da soggetti terzi idoneamente designati;
- coadiuvare ciascun Contitolare del trattamento e gli altri responsabili interni ed esterni eventualmente designati da ciascun Contitolare nell'attuazione di misure tecniche e organizzative adeguate per garantire un livello di sicurezza proporzionato al rischio, tenendo conto dello stato dell'arte e dei costi di attuazione, della natura e dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche;
- svolgere un ruolo di primaria interfaccia coadiuvando gli altri responsabili interni ed esterni della struttura informatica eventualmente designati di ciascun Contitolare, nel caso di incidenti/malfunzionamenti di qualsiasi genere che riguardino le utenze e preoccuparsi di erogare una corretta informazione verso gli utenti supportando il processo di indagine e diagnosi dei problemi ed essere in grado di produrre le necessarie informazioni a tal riguardo;
- eseguire direttamente o assicurarsi che vengano realizzate da soggetti terzi idoneamente designati le copie di sicurezza e ripristino, usando la massima riservatezza e discrezione affinché il processo venga svolto in conformità alle disposizioni di legge,
- assegnare e gestire il sistema di autenticazione informatica e quindi, fra le altre, generare, sostituire ed invalidare, in relazione agli strumenti ed alle applicazioni informatiche utilizzate, le parole chiave ed i codici identificativi personali da assegnare agli incaricati del trattamento dati, svolgendo anche la funzione di custode delle copie delle credenziali;
- procedere, più in particolare, alla disattivazione dei codici identificativi personali, in caso di perdita della qualità che consentiva all'utente o incaricato l'accesso all'elaboratore, oppure nel caso di mancato utilizzo dei codici identificativi personali per oltre 6 (sei) mesi;
- adottare adeguati strumenti software atti a garantire la massima misura di sicurezza ed utilizzando le conoscenze acquisite in base al progresso tecnico software, verificandone l'installazione, l'aggiornamento ed il funzionamento degli stessi in conformità alle linee guida AGID;
- adottare tutti i provvedimenti necessari ad evitare la perdita o la distruzione, anche solo accidentale, dei dati personali e provvedere al ricovero periodico degli stessi con copie di back-up, vigilando sulle procedure attivate dal titolare; l'Amministratore di sistema dovrà anche assicurarsi della qualità delle copie di back-up dei dati e della loro conservazione in luogo adatto e sicuro;
- indicare al personale competente o provvedere direttamente alla distruzione e smaltimento dei supporti informatici di memorizzazione logica o alla cancellazione dei dati per il loro reimpiego;
- cooperare nella predisposizione del registro dei trattamenti supportando adeguatamente i DPO di ciascun Contitolare per la parte concernente il sistema informatico ed il trattamento informatico dei dati;
- predisporre ed implementare le eventuali ulteriori misure di sicurezza imposte dalle misure minime di sicurezza AGID per il trattamento informatico dei dati comuni e particolari e per la conseguente tutela degli strumenti elettronici;
- coordinare insieme a ciascun Contitolare (e/o al RTD, qualora nominato) le attività operative degli autorizzati al trattamento nello svolgimento delle mansioni loro affidate per garantire un corretto, lecito

e sicuro trattamento dei dati personali nell'ambito del sistema informatico;

- collaborare con ciascun Contitolare (e/o al RTD, qualora nominato) e con i relativi DPO per l'attuazione delle prescrizioni impartite dal Garante;
- comunicare prontamente a ciascun Contitolare (e/o al RTD, qualora nominato) e ai relativi DPO qualsiasi situazione di cui sia venuta a conoscenza che possa compromettere il corretto trattamento informatico dei dati personali.

I Contitolari provvederanno a svolgere le dovute verifiche sulle attività compiute dall'Amministratore di sistema. È obbligo di quest'ultimo prestare a ciascun Contitolare la sua piena collaborazione per il compimento delle verifiche stesse; in ogni caso, è tenuto a predisporre, con cadenza annuale, una relazione scritta delle attività svolte in esecuzione delle incombenze affidatigli in forza del presente atto.

Responsabilità

Chiunque subisca un danno materiale o immateriale causato da una violazione del Regolamento ha il diritto di ottenere il risarcimento del danno da ciascun Contitolare o dal Responsabile. Il Responsabile risponde per il danno causato dal trattamento se non ha adempiuto gli obblighi posti dal Regolamento specificatamente diretti ai responsabili o ha agito in modo difforme o contrario rispetto alle legittime istruzioni impartite dai Contitolari nel presente atto.

In caso di richieste di risarcimento pervenute ai Contitolari congiuntamente o singolarmente, per violazioni compiute dal Responsabile, il Contitolare interessato dalla richiesta si riserva il diritto di rivalsa nei confronti del Responsabile stesso.

Per quanto riguarda le sanzioni imputabili da parte dell'Autorità Garante, fanno fede gli art. 82, 83 e 84 del Regolamento.

In caso di accertata violazione delle disposizioni del Regolamento o del presente contratto, ciascun Contitolare si riserva il diritto di mettere in atto le misure ritenute opportune nei confronti del Responsabile. Se la violazione si configurasse di particolare gravità è fatto salvo il diritto di ciascun Contitolare di richiedere la sospensione delle attività di trattamento e l'eventuale cessazione delle stesse con obbligo per il Responsabile di provvedere alla cancellazione e/o restituzione dei dati personali secondo quanto disciplinato alla lettera j che precede.

Durata

Le prescrizioni di cui al presente atto hanno decorrenza dall'ultima data di sottoscrizione e fino a quando continueranno a svilupparsi le obbligazioni contrattuali relative alla fornitura del sistema in oggetto.

Privacy by design e by default

In un'ottica di maggiore responsabilità dei soggetti incaricati del trattamento dei dati personali una delle novità più incisive che il legislatore europeo ha introdotto nella normativa sono i principi di privacy by design art 25.1 e privacy by default art 25.2 del regolamento. Tali principi garantiscono la protezione dei dati dalla fase di ideazione e progettazione di un trattamento o di un sistema e l'adozione di comportamenti che consentano di prevenire possibili problematiche.

Il principio di privacy by design ex art 25.1, descrive i criteri necessari a garantire la protezione dei dati personali sin dall'avvio del trattamento ed in particolare:

- la necessità di minimizzare l'uso del dato;
- la necessità di tutelare i diritti dell'interessato.

L'applicazione della privacy by default, ex art 25.2, implica, invece, l'adozione di misure tecniche ed organizzative che garantiscano, per impostazione predefinita, che siano trattati solo i dati necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. Non deve essere consentito l'accesso di dati personali a un numero indefinito di persone fisiche senza l'intervento di una persona fisica. Nell'applicazione dei principi della privacy by design e della privacy by default, in riferimento alle misure tecniche e organizzative, il considerando 78 del regolamento dispone che "al fine di poter dimostrare la conformità con il presente regolamento, il titolare del trattamento dovrebbe adottare politiche interne e attuare misure che soddisfino in particolare i principi della protezione dei dati fin dalla progettazione e della protezione dei dati di default." Inoltre il medesimo considerando 78 dispone che "i produttori dei prodotti dei servizi e delle applicazioni, in fase di sviluppo, progettazione selezione e utilizzo di applicazioni, servizi e prodotti basati sul trattamento di dati personali o che trattano dati personali per svolgere le loro funzioni i produttori dei prodotti, dei servizi e delle applicazioni

dovrebbero essere incoraggiati a tenere conto del diritto alla protezione dei dati allorché sviluppano e progettano tali prodotti, servizi e applicazioni e, tenuto debito conto dello stato dell'arte, a far sì che i titolari del trattamento e i responsabili del trattamento possano adempiere ai loro obblighi di protezione dei dati". In considerazione di quanto sopra esposto risulta necessario essere in grado di dimostrare in termini di accountability che i trattamenti di dati personali sviluppati mediante i prodotti o servizi forniti dalla vostra spett. azienda siano conformi ai citati principi di privacy by design e privacy by default.

Pertanto con la presente si chiede di avere indicazioni sulle funzioni in dotazione al sistema attraverso le quali i prodotti ed i servizi forniti dalla vostra azienda rispettino i principi della privacy by design e della privacy by default in particolar modo per quanto concerne:

- la minimizzazione nella durata del trattamento dati (art. 5.1.f - art. 25.2);
- la minimizzazione nella tipologia di dati trattati (art. 5.1.f - art. 25.2);
- la minimizzazione nella quantità di dati trattati (art. 5.1.f - art. 25.2);
- la minimizzazione negli accessi ai dati (art. 5.1.f - art. 25.2);
- la limitazione del trattamento (considerando 67 - art. 4.3 - art. 18);
- la cancellazione dei dati (art. 17);
- la possibilità di individuare una tempistica di conservazione dei dati (art. 13.2.a - art. 30.1.f).

Si richiede inoltre di avere indicazioni in merito alle eventuali modalità impiegate che consentano di:


- garantire la pseudonimizzazione dei dati (Considerando 26 – 28 – 29, Art. 4.5 - art. 25 - Art. 32.1 - art.40.2.d - art. 89.2);
- garantire l'anonimizzazione dei dati (Considerando 26);
- garantire la cifratura dei dati (art. 34.3.a).

Luogo e data _____

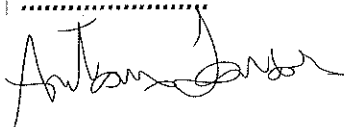
Firma del contitolare del trattamento dei dati personali ASST Fatebenefratelli Sacco

Firma per accettazione del responsabile del trattamento dei dati personali

Firma del contitolare del trattamento dei dati personali Proges Soc. Coop. Soc.



Firma dell'amministratore di sistema




Allegato A
ELENCO NOMINATIVO DEI SOGGETTI CHE OPERANO IN QUALITÀ DI AMMINISTRATORI DI SISTEMA
REDATTO DAL RESPONSABILE


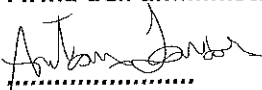
Cognome e Nome LOVICARIO ANTONIO

Il presente Allegato deve essere costantemente aggiornato dal responsabile in caso di modifiche e comunicato senza ritardo (e comunque non oltre le 48 ore) a ciascun Contitolare.

Luogo e data _____

Firma del contitolare del trattamento dei dati personali
.....

Firma per accettazione del responsabile del trattamento dei dati personali

.....

Firma del contitolare del trattamento dei dati personali

.....
Firma dell'amministratore di sistema

.....