Milano

Comune
di Milano

DIREZIONE Welfare e Salute
Area Territorialità e Sistema Integrato
Di Accesso ai Servizi Sociali Unità Milano
Welfare Emergenza

Atto per la disciplina del Responsabile del Trattamento dei dati personali Art. 28 GDPR

OGGETTO: SERVIZI DI TRASPORTO E ACCOMPAGNAMENTO – LOTTO 2 DI 2 – SERVIZIO DI TRASPORTO SERVIZIO DI TRASPORTO PER MINORI PRESSO STRUTTURE DI ACCOGLIENZA

IL DIRETTORE DI AREA E
RESPONSABILE DEL PROGETTO
Dott. Giuseppe Barbalace

Giuseppe
Barbalace
Comune di
Milano
Direttore
20.03.2025
16:49:07
GMT+01:00

Rev.	Data	Descrizione	Red.	Rev.	File
Rev. 0					

Atto per la disciplina del Responsabile

Oggetto: SERVIZI DI TRASPORTO E ACCOMPAGNAMENTO – LOTTO 2 DI 2 – SERVIZIO DI TRASPORTO PER MINORI PRESSO STRUTTURE DI ACCOGLIENZA

Premesso che

- Con deliberazione n. _____ del _____ sono state approvate le linee di indirizzo per _____;
- con determinazione dirigenziale n. _____ della Direzione/Area _____ in data ==/==/20==, il servizio relativo alla gara _____ è stato aggiudicato a (Inserire denominazione dell'aggiudicatario) con sede legale e domicilio fiscale in Via _____- 000000 (inserire CAP e città) - codice fiscale e partita I.V.A. n_____
- ai sensi dell'art.3.3 del Capitolato Speciale d'Appalto con verbale del RUP/Direttore dell'esecuzione in data _____ è stato richiesto l'avvio della prestazione in pendenza della stipulazione del contratto;
- il presente atto impegna già ora le parti e lo stesso verrà allegato parte integrante del contratto relativo al servizio sopra richiamato.
- l'esecuzione della prestazione comporta il trattamento dei dati personali da parte dell'appaltatore in qualità di "Responsabile" per il trattamento dei dati personali

Considerato che il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016, Regolamento Generale sulla protezione dei dati (di seguito GDPR):

- ha introdotto varie novità anche riguardo ai rapporti tra Titolare e Responsabile del trattamento e ai relativi strumenti di regolazione;
- in particolare l'art. 28 prevede di disciplinare con un contratto, o altro atto giuridico equivalente, i trattamenti effettuati dal Responsabile per conto del Titolare, che vincoli il Responsabile del trattamento al Titolare e definisca la durata del trattamento, la natura e lo scopo, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del Titolare.

Il Comune di Milano, in qualità di "Titolare del trattamento" (di seguito Titolare) a cui competono le decisioni in merito alle finalità e modalità del trattamento, rappresentato da rappresentato da Giuseppe Barbalace con sede in Milano, Via Sile, n. 8 ai sensi dell'art. 28 del GDPR

e

_____ , quale "Responsabile" del trattamento dei dati personali (di seguito Responsabile), rappresentato da _____**,** con sede in _____ , via/piazza _____ , n. ___

Convengono e stipulano quanto segue

1. Oggetto

Il presente Atto disciplina il trattamento dei dati personali da parte del Responsabile per conto del Titolare, nonché gli obblighi e i diritti delle Parti derivanti dal contratto di appalto citato in premessa. Il Responsabile fornisce i servizi al Titolare in relazione alla gestione delle attività relative all'affidamento del Servizio di trasporto e accompagnamento –Lotto 1 di 2 – Servizio di trasporto ed accompagnamento a favore degli ospiti dei Centri Diurni Disabili, dei Centri di Riabilitazione e dei Centri Socio Educativi.

Requisiti di professionalità

Secondo l'art. 28 del GDPR, quando un trattamento viene effettuato per conto del Titolare quest'ultimo ricorre unicamente a Responsabili del trattamento che forniscano piena garanzia del rispetto della normativa applicabile e che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate. Le incombenze oggetto del presente atto sono affidate al Responsabile in base alle dichiarazioni da questo fornite al Titolare in merito alle caratteristiche di esperienza, capacità e affidabilità previste dalla normativa applicabile.

Per **normativa applicabile** si intende l'insieme delle norme rilevanti in materia di protezione dei dati personali incluso il GDPR e inoltre, in ogni tempo, ogni linea guida, norma di legge, compresa la normativa nazionale di adeguamento al citato GDPR, nonché i provvedimenti del Garante per la protezione di dati, codice o provvedimento rilasciato o emesso dagli organi competenti o da altre autorità di controllo.

Il Responsabile con la sottoscrizione del presente **Atto** si dichiara disponibile, competente e di disporre una propria organizzazione per dare attuazione a quanto previsto, nonché in possesso dei requisiti di esperienza e capacità tali da fornire idonea garanzia del rispetto delle vigenti disposizioni in materia di trattamento dei dati personali, in particolare in termini di conoscenze specialistiche, affidabilità e risorse, per attuare misure tecniche e organizzative che soddisfino i requisiti del GDPR, compresa la sicurezza del trattamento per garantire la riservatezza e la protezione dei diritti degli interessati.

2. Ambito e limiti del trattamento dei dati

Il Responsabile è autorizzato ad effettuare esclusivamente le operazioni di trattamento necessarie per lo svolgimento delle attività concordate e descritte nel Capitolato Speciale d'Appalto che sinteticamente si riportano di seguito con l'indicazione della categoria dei dati:

Attività	Categorie di dati
Erogazione del servizio di trasporto per minori presso strutture di accoglienza.	- dati personali comuni, dati particolari

Si rinvia all'allegato 1 del presente Atto il dettaglio delle tipologie di dati trattati per l'esecuzione del servizio

A tal proposito, il Responsabile riconosce che le finalità del trattamento sono esclusivamente quelle individuate nel citato Capitolato Speciale d'Appalto. Il Responsabile ha accesso ai dati del Comune di Milano e quindi alle informazioni degli interessati per le attività necessarie e connesse allo svolgimento

delle attività descritte nei predetti atti, nei limiti di legge e di eventuali prescrizioni da parte del Comune medesimo.
Il Responsabile può accedere ai dati personali e ai dati particolari (ex articolo 9 GDPR) o relativi a condanne penali e reati (ex articolo 10 GDPR) degli utenti solo se la conoscibilità di tali informazioni è indispensabile per una specifica attività posta o da porre in essere; il Responsabile non può accedere ai predetti dati in via generale e/o massiva, ma solo in via puntuale. Nel caso di necessità di accesso massivo deve essere preventivamente autorizzato dal Titolare. Il Responsabile deve sempre garantire al Titolare l'accesso diretto ai dati attraverso il sistema di gestione utilizzato.

3. Dichiarazioni e compiti del Titolare

Il Titolare affida al Responsabile tutte le operazioni di trattamento dei dati personali necessarie per dare esecuzione al servizio in oggetto, e si impegna a comunicare qualsiasi variazione che dovesse rendersi necessaria nelle operazioni di trattamento.

Il Titolare precisa che i dati personali messi a disposizione del Responsabile, ivi compresi gli eventuali dati e categorie di dati particolari, sono connessi e strumentali all'esecuzione del compito di interesse pubblico strettamente correlato alla gestione del predetto servizio.

Il Titolare precisa, inoltre, che la raccolta dei dati personali da parte dal Responsabile deve avvenire nel rispetto della normativa applicabile ed in particolare del GDPR; i dati dovranno essere esatti ed aggiornati, pertinenti, completi e non eccedenti le finalità per le quali sono trattati.

Nell'ambito delle attività oggetto del presente Atto, il Titolare esercita funzioni di controllo utilizzando gli strumenti di verifica più opportuni rispetto all'attività: es. check list e verifiche periodiche tramite propri addetti presso la sede del Responsabile. A tal fine il Titolare informa il Responsabile con un preavviso minimo di tre giorni lavorativi, fatta comunque salva la possibilità di effettuare controlli a campione senza preavviso.

5. Obblighi e dichiarazioni del Responsabile

Il Responsabile, nell'espletamento della propria funzione, in forza del presente Atto, è tenuto a collaborare con il Titolare fornendo le informazioni e i documenti richiesti ed eventuali relazioni sui livelli di sicurezza dei sistemi e dei dati, sullo stato di attuazione della normativa, nonché sul modello organizzativo adottato e su certificazioni di sicurezza acquisite.

Il Responsabile si impegna a rispettare in ogni fase del trattamento le disposizioni previste dal GDPR e dalle norme in materia di protezione dei dati applicabili, in particolare le finalità, le modalità, le misure di sicurezza e gli ambiti di comunicazione dei trattamenti.

Tenendo conto della natura, dell'oggetto, del contesto e delle finalità del trattamento, nonché del rischio di varia probabilità e gravità per i diritti e per le libertà delle persone fisiche, il Responsabile, al fine di proteggere i dati personali, siano essi trattati con strumenti elettronici e/o cartacei, mette in atto misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato ai rischi, inclusi quelli di:

- distruzione, perdita, modifica, divulgazione non autorizzata o accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati;

- trattamento dei dati non consentito o non conforme alle finalità delle operazioni di trattamento definite dal Titolare.

Il Responsabile si impegna altresì a trattare i dati personali solo per conto del Titolare e limitatamente alle attività di trattamento strettamente necessarie per l'esecuzione del servizio in oggetto, in conformità con le istruzioni impartite dal Titolare. Qualora il Responsabile non sia in grado di garantire per qualsiasi motivo la suddetta conformità, informa tempestivamente il Titolare che ha il diritto di sospendere l'attività e l'elaborazione dei dati e, nei casi di particolare gravità motivati per iscritto dal Titolare, di risolvere il Contratto.

Nel caso in cui le operazioni di trattamento avvengano in locali presso la sede del Responsabile o in locali nella propria disponibilità, il Responsabile in relazione a quanto previsto dal precedente punto 4 – ultimo paragrafo - riconosce al Titolare il diritto di accedere ai predetti locali. Per contro il Titolare si impegna ad utilizzare le informazioni raccolte durante le operazioni di verifica solo per tali finalità.
Nel caso in cui le operazioni di trattamento di dati su supporto cartaceo avvengano in locali presso la sede del Titolare, la responsabilità circa l'adozione delle misure di sicurezza di tipo fisico sarà in capo al Responsabile solo durante la sua permanenza presso gli Uffici del Titolare.

Fermo restando quanto previsto ai precedenti punti, il Responsabile dichiara di aver ricevuto, esaminato, condiviso e compreso le istruzioni impartite dal Titolare con il presente Atto e con i documenti connessi, nonché quelle di seguito indicate alle quali dovrà attenersi nell'esecuzione dell'incarico.

6. Ulteriori obblighi e istruzioni per il Responsabile
Il Responsabile, nell'esercizio delle proprie funzioni è tenuto, anche con riguardo alle persone autorizzate al trattamento che collaborano con la sua organizzazione, ad osservare gli obblighi inerenti le misure di sicurezza previste dalle norme in materia e a fornire assistenza al Titolare per garantirne il rispetto.

Il Responsabile, nell'ambito dei trattamenti effettuati presso le proprie sedi o presso i locali nella sua piena ed esclusiva disponibilità e/o con propri strumenti informatici, implementa le misure di sicurezza definite puntualmente **nell'Allegato 1** al fine di garantire:

- la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
- la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico.

Nell'ambito dei trattamenti effettuati presso le proprie sedi e/o con propri strumenti informatici il Responsabile fornisce, la documentazione relativa al piano di sicurezza per la gestione degli eventi di data breach, con la descrizione delle misure di sicurezza adottate in rapporto all'eventuale violazione dei dati; in particolare predispone e aggiorna un registro che dettagli, in caso di eventuali *data breach*, la natura delle violazioni, gli interessati coinvolti, le possibili conseguenze.

Il Responsabile è tenuto ad informare il Titolare del trattamento, immediatamente e senza ingiustificato ritardo appena avutane conoscenza, in ordine a qualsiasi violazione di dati personali anche se intervenuta presso i propri Sub-Responsabili qualora nominati. Il Responsabile dovrà assicurare il pieno supporto al Titolare del trattamento e all'Autorità di controllo per ottemperare alle obbligazioni previste dalle norme

vigenti (ad esempio notifica delle violazioni di dati personali all'Autorità di controllo; laddove applicabile, comunicare la violazione di dati personali agli interessati).

Il Responsabile è tenuto inoltre ad adottare in accordo con il Titolare ulteriori misure finalizzate a circoscrivere gli effetti negativi dell'evento e ripristinare la situazione precedente.

Il Responsabile inoltre:

1. adotta le misure di cui all'art. 25 del GDPR rubricato "Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita" (cd. "Privacy by Default" e "by Design") ovvero misure tecniche ed organizzative adeguate garantendo che, per impostazione predefinita, vengano raccolti e trattati solo i dati strettamente necessari al raggiungimento delle finalità stabilite e limitando l'accesso ad un numero definito di persone preventivamente autorizzate;
2. applica, se del caso, misure come l'anonimizzazione, la cifratura la pseudonimizzazione intesa come modalità di "riduzione della correlabilità di un insieme di dati all'identità originaria di una persona interessata";
3. garantisce il rispetto degli obblighi di cui agli art. 32-36 del GDPR tenendo conto della natura del trattamento e delle informazioni a propria disposizione;
4. tiene un Registro ai sensi dell'art. 30 del GDPR di tutte le categorie di attività relative al trattamento svolte per conto del Titolare;
5. non comunica a terzi né diffonde i dati di cui viene a conoscenza, salvo che tali operazioni siano autorizzate dal Titolare del trattamento e previste da norme di legge o di regolamento nazionali o dell'Unione Europea;
6. collabora a redigere l'informativa ai sensi dell'art. 13 e 14 del GDPR con il Titolare, con il quale concorda le modalità con cui fornirla agli interessati;
7. non effettua di propria iniziativa alcuna operazione di trattamento diversa da quelle previste se non autorizzata dal Titolare;
8. non trasferisce i dati trattati per conto del Titolare al di fuori dello Spazio Economico Europeo senza autorizzazione scritta da parte del Titolare stesso;
9. adotta adeguati sistemi per assicurare i diritti riconosciuti agli interessati dal GDPR;
10. informa tempestivamente il Titolare in merito ad eventuali richieste inviate da parte degli interessati
11. garantisce al Titolare - se da questo richiesto - la tutela dei diritti innanzi al Garante per la protezione dei dati personali in caso di eventuali contenziosi rispetto al servizio offerto;
12. collabora con il Titolare per il rispetto di eventuali prescrizioni emesse dall'Autorità Garante o dall'Autorità Giudiziaria in relazione al trattamento dei dati;
13. informa tempestivamente il Titolare del trattamento di qualsiasi richiesta legalmente vincolante per la divulgazione dei dati personali da parte di un'Autorità Giudiziaria salvo laddove diversamente vietato per rilevanti motivi di interesse pubblico;
14. informa immediatamente il Titolare a mezzo e-mail all'indirizzo e-mail dpo@comune.milano.it in caso di ispezioni, di richiesta di informazioni e di documentazione da parte dell'Autorità Garante;
15. realizza tutto quanto sia utile e/o necessario per garantire gli adempimenti di tutti gli obblighi previsti dal GDPR.

Inoltre, qualora i trattamenti dovessero presentare un rischio elevato per la dignità e la libertà delle persone, il Responsabile assiste e supporta il Titolare nella valutazione di impatto (data protection impact assessment – DPIA) e nell'eventuale consultazione preliminare all'Autorità di Controllo, laddove applicabile.

Il Titolare, in funzione di eventuali evoluzioni tecnologiche e/o normative, può richiedere ulteriori misure di sicurezza rispetto a quelle adottate dal Responsabile. In tal caso il Titolare fornirà adeguate istruzioni con sufficiente preavviso e concorda con il Responsabile i tempi per attuarle.

Il Responsabile al termine delle attività connesse alla propria funzione e delle prestazioni contrattualmente previste consegna al Titolare:

- tutte le informazioni raccolte con qualsiasi modalità, cartacea e/o elettronica;
- i supporti rimovibili eventualmente utilizzati in cui sono memorizzati i dati;
- distrugge tutte le informazioni registrate su supporto fisso, documentando per iscritto l'adempimento di tale operazione. Il Titolare si riserva il diritto di effettuare controlli e verifiche al fine di accertare la veridicità delle dichiarazioni rese.

7. Persone autorizzate al trattamento

Il Responsabile nell'ambito della propria organizzazione individua e autorizza le persone a trattare i dati e contestualmente fornisce loro, per iscritto, le istruzioni in merito ai trattamenti, con particolare riferimento alle modalità e alle operazioni che possono essere svolte sui dati in attuazione a quanto previsto dalle norme in materia e dal presente Atto. I nominativi delle persone autorizzate al trattamento saranno forniti al Titolare se richiesto.

Il Responsabile mette in atto le relative misure per consentire alle persone autorizzate di accedere ai soli dati la cui conoscenza sia strettamente necessaria per adempiere ai compiti assegnati e avrà cura di fornire a tali persone che, per mansioni e funzioni, avranno accesso ai dati personali comuni, particolari e relativi a condanne penali o reati, tutte le indicazioni e le specifiche regole comportamentali affinché i trattamenti effettuati siano conformi ai principi di pertinenza, non eccedenza e indispensabilità.

Al riguardo, il Responsabile verifica che le persone autorizzate: a) applichino tutte le disposizioni in materia di sicurezza relativa alla custodia delle parole chiavi (trattamenti elettronici); b) conservino in luogo sicuro i supporti non informatici contenenti atti o documenti con categorie particolari di dati o la loro riproduzione, adottando contenitori con serratura (trattamenti cartacei di dati).

Il Responsabile vincola le predette persone alla riservatezza e al rispetto di tale obbligo anche per il periodo successivo all'estinzione del rapporto di collaborazione intrattenuto con il Responsabile, in relazione alle operazioni di trattamento da esse eseguite.

Il Responsabile sottopone le persone autorizzate ad interventi formativi e di aggiornamento periodico o approfondimento per renderle edotte dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure adottate.

8. Sub-Responsabili

Con il presente Atto, il Responsabile si impegna ad informare il Titolare di altri eventuali ulteriori responsabili del trattamento impegnati nella prestazione del servizio in oggetto.

Il Responsabile in caso di ricorso a sub-responsabili, si impegna a selezionarli tra soggetti che per esperienza, capacità e affidabilità forniscano garanzie sufficienti per mettere in atto le misure tecniche e organizzative adeguate descritte nell'**Allegato 1 "**Misure di sicurezza" e allegato 1bis in modo tale che il trattamento soddisfi i requisiti di cui alla normativa applicabile e garantisca la tutela dei diritti degli interessati. Nell'ambito del presente Atto, il Titolare fornirà un'autorizzazione scritta al Responsabile affinché lo stesso possa ricorrere a eventuali sub responsabili preventivamente comunicati compilando **l'Allegato 2** da aggiornare sistematicamente se necessario.
Il Responsabile si impegna altresì ad informare il Titolare di eventuali modifiche o sostituzioni riguardanti i sub-responsabili, fermo restando la possibilità da parte del Titolare di opporsi alle predette modifiche o sostituzioni

Il Responsabile si impegna a stipulare specifici contratti, o altri atti giuridici, con i sub-responsabili che descrivano analiticamente i loro compiti e impongano a tali soggetti il rispetto degli stessi obblighi imposti dal Titolare al Responsabile, affinché il trattamento soddisfi i requisiti previsti dalle norme applicabili in materia di protezione dei dati personali e dai provvedimenti emanati dall'Autorità di Controllo. I contratti dovranno prevedere a carico dei sub-responsabili processi di assessment mirati e il rispetto delle istruzioni del Titolare.

I sub-responsabili dovranno seguire le istruzioni impartite dal Titolare al Responsabile originario, il quale dovrà farsi carico di fornirle ai sub-responsabili. Il Responsabile "originario" è tenuto a monitorare le debite prestazioni e gli adempimenti assegnati ai sub-responsabili.

Il Responsabile del trattamento rimane pienamente responsabile nei confronti del Titolare per l'adempimento degli obblighi dei sub-responsabili. Pertanto qualora il sub-responsabile non osservi i propri obblighi, il Responsabile: (i) conserva nei confronti del Titolare l'intera responsabilità dell'adempimento degli obblighi dei sub-responsabili coinvolti; (ii) si impegna a manlevare e tenere indenne il Titolare da qualsiasi danno, pretesa, risarcimento, e/o sanzione possa derivare al Titolare dalla mancata osservanza di tali obblighi e più in generale dalla violazione della normativa sulla tutela dei dati personali da parte del Responsabile e dei suoi sub-responsabili.

9. Amministratori di sistema

Il Responsabile si obbliga ad applicare e a rispettare il provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008 e successive modifiche ed integrazioni recante disciplina in materia di amministratori di sistema impegnandosi, in particolare, a conservare direttamente e specificamente gli estremi identificativi delle persone fisiche preposte alle funzioni di amministratore di sistema e a fornirli prontamente al Titolare su richiesta del medesimo.
Il Responsabile si obbliga altresì a verificare, con cadenza almeno annuale e comunque ogni qualvolta lo richieda il Titolare, l'operato degli amministratori di sistema al fine di controllare la rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti previsti dalle norme vigenti.

10. Responsabilità

Il Responsabile risponde, ai sensi degli artt. 82, 83 e 84 del GDPR, per il danno causato dal trattamento se non ha adempiuto agli obblighi del Regolamento specificamente diretti ai Responsabili del trattamento e qualora abbia agito in modo difforme o contrario alle legittime istruzioni del Titolare.

11. Comunicazioni tra le parti
Ciascuna parte (Titolare e Responsabile) informerà l'altra tempestivamente di ogni provvedimento dell'Autorità di Controllo connesso al presente Atto. In particolare il Responsabile avvisa immediatamente il Titolare in caso di ispezioni, di richiesta di informazioni e di documentazione da parte dell'Autorità di Controllo.

12 Richieste degli interessati
Su espressa richiesta del Titolare, nella misura in cui ciò sia possibile, il Responsabile fornisce riscontro alle eventuali istanze degli interessati nei termini previsti dal GDPR. Il Responsabile prima di provvedere sottopone al Titolare la risposta da fornire in merito al trattamento dei dati

13. Corrispettivo e spese
L'esecuzione delle attività e dei compiti di cui al presente atto non genera il diritto ad alcun compenso a favore del nominato Responsabile, in quanto le predette attività e compiti sono svolti nell'ambito del Capitolato Speciale d'appalto nei quali è già stata definita l'intera valutazione economica del rapporto tra le Parti.

14. Cessazione e Revoca

Il presente Atto cessa automaticamente di produrre effetti al termine delle attività previste dall'appalto di servizio in oggetto, ovvero automaticamente, in caso di esercizio del diritto di recesso di cui all'articolo 6.4 del Capitolato Speciale d'Appalto.

Il Titolare può revocare l'incarico in caso di svolgimento delle funzioni non conforme alle istruzioni fornite, nonché per la sopravvenuta perdita dei requisiti di cui all'art. 28 del GDPR o per esigenze di interesse pubblico.

Letto, approvato e sottoscritto.

Milano, _____

Il Comune di Milano
Titolare del Trattamento
Rappresentato da:

Per accettazione e, consapevole delle responsabilità previste dal D.P.R. n. 445/2000, dichiarando di operare in conformità al GDPR e al D. Lgs. n.196/2003 come modificato dal D. Lgs. n. 101/2018

La Ditta/Società
Rappresentata da:

Allegato 1 Misure di sicurezza

Le attività di trattamento sono effettuate al fine di garantire la gestione dei procedimenti finalizzati allo svolgimento del Servizio di trasporto e accompagnamento –Lotto 1 di 2 – Servizio di trasporto ed accompagnamento a favore degli ospiti dei Centri Diurni Disabili, dei Centri di Riabilitazione e dei Centri Socio Educativi

Erogazione del servizio di trasporto ed accompagnamento a favore degli ospiti dei centri diurni disabili, dei centri di riabilitazione e dei centri socio educativi.

Categorie di Interessati

I Dati Personali trattati riguardano le seguenti categorie di Interessati:

- minori accompagnati presso strutture di accoglienza

Tipologia di Dati Personali

I Dati Personali trattati per conto del Titolare riguardano le seguenti categorie di Dati Personali:

- CODICE FISCALE
- CONTATTI E-MAIL
- DATI ANAGRAFICI – Nome, cognome (art. 4 punto 1 Regolamento)
- DATI DI FAMIGLIA O SITUAZIONI PERSONALE
- RECAPITO (CONTATTI TELEFONICI) /INDIRIZZO
- RESIDENZA

I dati forniti dal Titolare al Responsabile sono:

X in chiaro

☐ criptati

In relazione al contesto e ai rischi analizzati il Responsabile nell'ambito delle attività contrattualmente previste garantisce di applicare le seguenti misure di sicurezza come da allegato 1*bis*

Allegato 2 – Elenco dei sub-responsabili

Ubicazione del titolare	Responsabile	Sub-responsabile

L'elenco dei sub-responsabili è oggetto di aggiornamento sistematico ed è sottoposto al Titolare per le valutazioni e l'eventuale opposizione di ulteriori sub-responsabili

Comune di Milano	**Vigilanza e controllo sull'operato dei Responsabili del Trattamento dei dati personali Art. 28 GDPR - Misure di sicurezza** **ALLEGATO 1BIS**	
ID misura	**Misura per designazione**	**Riferimenti a standard**
DP-ID.AM-7	I ruoli e le responsabilità inerenti al trattamento e la protezione dei dati personali per tutto il personale e per eventuali terze parti rilevanti (es. fornitori, clienti, partner) devono essere definiti e resi noti	· GDPR - Artt. 24, 26-29, 37-39 · D.Lgs. 30/6/2003 n. 196 Artt. 2-quaterdecies, 2-quinquiesdecies, 2-sexiesdecies · ISO/IEC 29100:2011 4.2, 4.3, 5.10
DP-ID.AM-8	I trattamenti di dati personali devono essere identificati e catalogati	· GDPR - Art. 30 · ISO/IEC 29100:2011 4.4
ID.RA-5	Le minacce, le vulnerabilità, le relative probabilità di accadimento e conseguenti impatti devono essere utilizzati per determinare il rischio	· CIS CSC 4 · COBIT 5 APO12.02 · ISO/IEC 27001:2013 A.12.6.1 · NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-16 · Misure Minime AgID ABSC 4.8.1
DP-ID.DM-2:	I processi riguardanti l'informazione dell'interessato in merito al trattamento dei dati devono essere definiti, implementati e documentati	· GDPR - Artt. 12-14 · ISO/IEC 29100:2011 5.2, 5.8 · ISO/IEC 29151:2017 A.3, A.9 · ISO/IEC 27018:2014 A.1, A.7
DP-ID.DM-3	I processi di raccolta e revoca del consenso dell'interessato al trattamento di dati devono essere definiti, implementati e documentati	· GDPR - Artt. 7, 8 · D.Lgs. 30/6/2003 n. 196 Art. 2-quinquies · ISO/IEC 29100:2011 5.2 · ISO/IEC 29151:2017 A.3 · ISO/IEC 27018:2014 A.1
DP-ID.DM-4	I processi per l'esercizio dei diritti (accesso, rettifica, cancellazione, ecc.) dell'interessato devono essere definiti, implementati e documentati	· GDPR - Art 15-22 · D.Lgs. 30/6/2003 n. 196 Art. 2-terdecies · ISO/IEC 29100:2011 5.4, 5.5, 5.6, 5.7, 5.8, 5.9 · ISO/IEC 29151:2017 A.5, A.6, A.7, A.8, A.9, A.10 · ISO/IEC 27018:2014 A.3, A.4, A.5, A.6, A.7, A.8
ID.GV-1	Una policy di cybersecurity deve essere identificata e resa nota	· CIS CSC 19 · COBIT 5 APO01.03, APO13.01, EDM01.01, EDM01.02 · ISA 62443-2-1:2009 4.3.2.6 · ISO/IEC 27001:2013 A.5.1.1 · NIST SP 800-53 Rev. 4 -1 controls from all security control families · D.Lgs. 18/5/2018 n. 65 Artt. 13(2), 15(2)
ID.GV-2	Ruoli e responsabilità inerenti la cybersecurity devono essere coordinati ed allineati con i ruoli interni ed i partner esterni	· CIS CSC 19 · COBIT 5 APO01.02, APO10.03, APO13.02, DSS05.04 · ISA 62443-2-1:2009 4.3.2.3.3 · ISO/IEC 27001:2013 A.6.1.1, A.7.2.1, A.15.1.1 · NIST SP 800-53 Rev. 4 PS-7, PM-1, PM-2
ID.AM-1	I sistemi e gli apparati fisici in uso nell'organizzazione devono essere censiti	· CIS CSC 1 · COBIT 5 BAI09.01, BAI09.02 · ISA 62443-2-1:2009 4.2.3.4 · ISA 62443-3-3:2013 SR 7.8 · ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 · NIST SP 800-53 Rev. 4 CM-8, PM-5 · Misure Minime AgID ABSC 1
ID.AM-2	Le piattaforme e le applicazioni software in uso nell'organizzazione devono essere censite	· CIS CSC 2 · COBIT 5 BAI09.01, BAI09.02, BAI09.05 · ISA 62443-2-1:2009 4.2.3.4 · ISA 62443-3-3:2013 SR 7.8 · ISO/IEC 27001:2013 A.8.1.1, A.8.1.2, A.12.5.1 · NIST SP 800-53 Rev. 4 CM-8, PM-5 · Misure Minime AgID ABSC 2
ID.AM-3	I flussi di dati e comunicazioni inerenti l'organizzazione devono essere identificati	· CIS CSC 12 · COBIT 5 DSS05.02 · ISA 62443-2-1:2009 4.2.3.4 · ISO/IEC 27001:2013 A.13.2.1, A.13.2.2 · NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8 · Misure Minime AgID ABSC 5.1.4, 13.3.1, 13.4.1, 13.6, 13.7.1, 13.8.1
PR.AC-CDM1	Le credenziali di accesso ai sistemi devono essere nominative e le password devono sottostare a una policy che imponga la definizione di password con una complessità minima tale da renderle sicure	Controllo inserito dal Comune di Milano
PR.AC-1	Le identità digitali e le credenziali di accesso per gli utenti, i dispositivi e i processi autorizzati devono essere amministrate, verificate, revocate e sottoposte a audit sicurezza	· CIS CSC 1, 5, 15, 16 · COBIT 5 DSS05.04, DSS06.03 · ISA 62443-2-1:2009 4.3.3.5.1 · ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9 · ISO/IEC 27001:2013 A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.6, A.9.3.1, A.9.4.2, A.9.4.3 · NIST SP 800-53 Rev. 4 AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11 · D.Lgs. 18/5/2018 n. 65 Artt. 12(1)-(3), 14(1)-(3), 14(13) · Misure Minime AgID ABSC 5.6.1, 5.7, 5.8.1, 5.11 · GDPR - Artt. 25, 32 · ISO/IEC 29100:2011 5.11

ID misura	Misura per designazione	Riferimenti a standard
PR.AC-2	L'accesso fisico alle risorse deve essere protetto e amministrato	· COBIT 5 DSS01.04, DSS05.05 · ISA 62443-2-1:2009 4.3.3.3.2, 4.3.3.3.8 · ISO/IEC 27001:2013 A.11.1.1, A.11.1.2, A.11.1.3, A.11.1.4, A.11.1.5, A.11.1.6, A.11.2.1, A.11.2.3, A.11.2.5, A.11.2.6, A.11.2.7, A.11.2.8 · NIST SP 800-53 Rev. 4 PE-2, PE-3, PE-4, PE-5, PE-6, PE-8 · D.Lgs. 18/5/2018 n. 65 Artt. 12(1)-(3), 14(1)-(3), 14(13) · Misure Minime AgID ABSC 5.11.2, 10.4.1 · GDPR - Art. 32 · ISO/IEC 29100:2011 5.11
PR.AT-1	Tutti gli utenti devono essere informati e addestrati	· CIS CSC 17, 18 · COBIT 5 APO07.03, BAI05.07 · ISA 62443-2-1:2009 4.3.2.4.2 · ISO/IEC 27001:2013 A.7.2.2, A.12.2.1 · NIST SP 800-53 Rev. 4 AT-2, PM-13 · D.Lgs. 18/5/2018 n. 65 Artt. 12(1)-(3), 14(1)-(3), 14(13) · Misure Minime AgID ABSC 8.7.2, 8.7.3, 8.7.4
PR.AT-2	Gli utenti dotati di privilegi (es. amministratori di sistema) devono essere coscienti dei propri ruoli e responsabilità	· CIS CSC 5, 17, 18 · COBIT 5 APO07.02, DSS05.04, DSS06.03 · ISA 62443-2-1:2009 4.3.2.4.2, 4.3.2.4.3 · ISO/IEC 27001:2013 A.6.1.1, A.7.2.2 · NIST SP 800-53 Rev. 4 AT-3, PM-13 · D.Lgs. 18/5/2018 n. 65 Artt. 12(1)-(3), 14(1)-(3), 14(13) · Misure Minime AgID ABSC 5.2.1, 5.6.1, 5.7.1, 5.7.2, 5.7.3, 5.7.6, 5.8.1, 5.9.1, 5.10.3, 5.10.4, 5.11.1
PR.AT-3	Tutte le terze parti (es. fornitori, clienti, partner) devono essere coscienti dei propri ruoli e responsabilità	· CIS CSC 17 · COBIT 5 APO07.03, APO07.06, APO10.04, APO10.05 · ISA 62443-2-1:2009 4.3.2.4.2 · ISO/IEC 27001:2013 A.6.1.1, A.7.2.1, A.7.2.2 · NIST SP 800-53 Rev. 4 PS-7, SA-9, SA-16 · D.Lgs. 18/5/2018 n. 65 Artt. 12(1)-(3), 14(1)-(3), 14(13)
PR.PT-CDM1	Tutti i dispositivi client (postazioni di lavoro e dispositivi mobili) devono essere dotati di software per garantire la endpoint security (antivirus o antimalware)	Controllo inserito dal Comune di Milano
DE.CM-4	Il codice malevolo deve essere rilevato	· CIS CSC 4, 7, 8, 12 · COBIT 5 DSS05.01 · ISA 62443-2-1:2009 4.3.4.3.8 · ISA 62443-3-3:2013 SR 3.2 · ISO/IEC 27001:2013 A.12.2.1 · NIST SP 800-53 Rev. 4 SI-3, SI-8 · Misure Minime AgID ABSC 8.1.1, 8.2.2, 8.2.3, 8.5, 8.6.1, 8.7.2, 8.7.3, 8.7.4, 8.8.1, 8.9, 8.10.1, 8.11.1
PR.DS-3	I processi di trasferimento fisico, di rimozione e di distruzone dei dispositivi atti alla memorizzazione di dati devono essere gestititi attenendosi a un processo formale	· CIS CSC 1 · COBIT 5 BAI09.03 · ISA 62443-2-1:2009 4.3.3.3.9, 4.3.4.4.1 · ISA 62443-3-3:2013 SR 4.2 · ISO/IEC 27001:2013 A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.5, A.11.2.7 · NIST SP 800-53 Rev. 4 CM-8, MP-6, PE-16 · D.Lgs. 18/5/2018 n. 65 Artt. 12(1)-(3), 14(1)-(3), 14(13) · GDPR - Art. 32 · ISO/IEC 29100:2011 5.11
PR.IP-4	I backup delle informazioni devono essere eseguiti, amministrati e verificati	· CIS CSC 10 · COBIT 5 APO13.01, DSS01.01, DSS04.07 · ISA 62443-2-1:2009 4.3.4.3.9 · ISA 62443-3-3:2013 SR 7.3, SR 7.4 · ISO/IEC 27001:2013 A.12.3.1, A.17.1.2, A.17.1.3, A.18.1.3 · NIST SP 800-53 Rev. 4 CP-4, CP-6, CP-9 · D.Lgs. 18/5/2018 n. 65 Artt. 12(1)-(3), 14(1)-(3), 14(13) · Misure Minime AgID ABSC 10.1, 10.2.1, 10.4.1 · GDPR - Art. 32 · ISO/IEC 29100:2011 5.11
PR.IP-6	I dati devono essere distrutti in conformità con le policy	· COBIT 5 BAI09.03, DSS05.06 · ISA 62443-2-1:2009 4.3.4.4.4 · ISA 62443-3-3:2013 SR 4.2 · ISO/IEC 27001:2013 A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7 · NIST SP 800-53 Rev. 4 MP-6 · D.Lgs. 18/5/2018 n. 65 Artt. 12(1)-(3), 14(1)-(3), 14(13) · GDPR - Art. 5, 17, 32 · ISO/IEC 29100:2011 5.11
PR.IP-9	In caso di incidente/disastro, devono essere attivi e amministrati piani di risposta (Incident Response e Business Continuity) e recupero (Incident Recovery e Disaster Recovery)	· CIS CSC 19 · COBIT 5 APO12.06, DSS04.03 · ISA 62443-2-1:2009 4.3.2.5.3, 4.3.4.5.1 · ISO/IEC 27001:2013 A.16.1.1, A.17.1.1, A.17.1.2, A.17.1.3 · NIST SP 800-53 Rev. 4 CP-2, CP-7, CP-12, CP-13, IR-7, IR-8, IR-9, PE-17 · D.Lgs. 18/5/2018 n. 65 Artt. 12(1)-(3), 14(1)-(3), 14(13) · Misure Minime AgID ABSC 10.4.1 · GDPR - Art. 32 · ISO/IEC 29100:2011 5.11

ID misura	Misura per designazione	Riferimenti a standard
PR.PT-1	Deve esistere ed essere attuata una policy per definire, implementare e revisionare i log dei sistemi	· CIS CSC 1, 3, 5, 6, 14, 15, 16 · COBIT 5 APO11.04, BAI03.05, DSS05.04, DSS05.07, MEA02.01 · ISA 62443-2-1:2009 4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4 · ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12 · ISO/IEC 27001:2013 A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1 · NIST SP 800-53 Rev. 4 AU Family · D.Lgs. 18/5/2018 n. 65 Artt. 12(1)-(3), 14(1)-(3), 14(13) · Misure Minime AgID ABSC 5.5.1 · GDPR - Art. 32 · ISO/IEC 29100:2011 5.11
DE.DP-3	I processi di monitoraggio devono essere testati	· COBIT 5 APO13.02, DSS05.02 · ISA 62443-2-1:2009 4.4.3.2 · ISA 62443-3-3:2013 SR 3.3 · ISO/IEC 27001:2013 A.14.2.8 · NIST SP 800-53 Rev. 4 CA-2, CA-7, PE-3, SI-3, SI-4, PM-14 · D.Lgs. 18/5/2018 n. 65 Art. 14(2)-(3)
ID.BE-5	I requisiti di resilienza a supporto della fornitura di servizi critici per tutti gli stati di esercizio (es. sotto stress/attacco, in fase di recovery, normale esercizio) devono essere identificati e resi noti	· COBIT 5 BAI03.02, DSS04.02 · ISO/IEC 27001:2013 A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 · NIST SP 800-53 Rev. 4 CP-2, CP-11, SA-13, SA-14
DP-ID.DM-1	Il ciclo di vita dei dati deve essere definito e documentato	· GDPR - Art. 5,6,9-11, 30