CONTRATTO TRA

COMUNE DI PESARO TITOLARE DEL TRATTAMENTO DI DATI E COOPERATIVA/ASSOCIAZIONE/DITTA…….. RESPONSABILE DEL TRATTAMENTO DATI IN QUALITA' DI OPERATORE AUTORIZZATO ALL'ACCOGLIENZA RESIDENZIALE RIVOLTA A MINORI / DONNE ANCHE CON FIGLI MINORI / ADULTI/E IN DIFFICOLTÀ SOCIALE E/O CON PROBLEMATICHE DI NATURA PSICO-SOCIALE– ISCRITTA NELL'ELENCO COMUNALE APERTO COME DA AVVISO DEL 23/05/2018

Allegato al contratto
Reg. n……./ 2018

L'anno…….il giorno ……..del mese di ……..presso gli uffici del Servizio Politiche Sociali ubicati a Pesaro in Via Mameli, n. 9;

Richiamato il Regolamento (UE) 2016/679 del Parlamento europeo ed in particolare le clausole che disciplinano i rapporti e le reciproche responsabilità tra Titolare del Trattamento di dati a carattere personale e il Responsabile del Trattamento;

Vista la determinazione nr. 1238 del 22 maggio 2018 con la quale è stato approvato l'Avviso pubblico per il rinnovo dell'Elenco comunale aperto degli Operatori autorizzati alla gestione di strutture residenziali di accoglienza e Pronta Accoglienza a favore di minori rinvenuti nel territorio comunale/minori allontanati dalla famiglia, donne anche con figli minori, adulti/e in difficoltà sociale e/o con problematiche di natura psico-sociale con validità per il periodo luglio 2018 - giugno 2020;

Richiamata, inoltre**,** la determinazione n. 1651 del 28/06/2018 con la quale è stato approvato in prima istanza, il nuovo Elenco comunale aperto sopra indicato, pubblicato nel sito istituzionale dell'Ente alla Sezione Amministrazione Trasparente sotto sezione "Bandi di gara, contratti" e nell'area Tematica "Servizi Sociali" - "Inserimento in Elenchi aperti" ,costantemente aggiornato con le nuove istanze che perverranno nel periodo di validità dell'Elenco stesso come sopra indicato;

TRA

Comune di Pesaro con sede legale in Piazza del Popolo, n. 1, C.F 00272430414 rappresentato da [……...]
(qui di seguito, "il Titolare del trattamento")

E

Società/Cooperativa/Associazione……..con sede a …… in via ……. n. .., codice fiscale ……e numero di iscrizione al Registro delle Imprese C.C.I.A.A.: …….., oppure iscritta all'Albo Regionale delle organizzazioni di volontariato al nr…….. in data…….., rappresentato da Sig./Sig.ra ……., nato/a a ……..(..) il ……il/la quale interviene al presente atto non in proprio, ma nella sua qualità di Presidente del Consiglio di Amministrazione dell'Impresa stessa;
(qui di seguito, "il Responsabile del trattamento")

La premessa forma parte integrale e sostanziale del presente atto;
Con il presente atto redatto in duplice originale

SI CONVIENE E SI STIPULA QUANTO SEGUE

Art. 1 - Oggetto
Oggetto del presente contratto è definire le modalità nelle quali l'Impresa Incaricata sopra generalizzata, in **qualità di Responsabile del trattamento** si impegna ad effettuare per conto del **Comune di Pesaro in qualità di Titolare del trattamento,** le operazioni di trattamento dei dati personali indicati al successivo articolo 2, relativamente al servizio specificato in oggetto.
Nel quadro delle loro relazioni contrattuali, le parti si impegnano a rispettare la regolamentazione in vigore applicabile al trattamento dei dati a carattere personale e, in particolare, il regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 applicabile dal 25 maggio 2018.

Art. 2 - Descrizione delle prestazioni del Responsabile del trattamento
Il Responsabile del trattamento è autorizzato a trattare per conto del Titolare del trattamento, i dati a carattere personale (dati personali) necessari per fornire i servizi connessi all'accoglienza presso strutture residenziali regolarmente autorizzate all'attività ai sensi di legge.

La finalità o le finalità del trattamento sono:
Tutela a favore di minori che versino in situazioni di disagio familiare / sociale o che si trovino in situazioni multiproblematiche, o in stato di abbandono.
Sostegno e tutela alla persona e al nucleo familiare. Pronto Intervento Sociale.
Interventi, anche di carattere socio sanitario volti all'assistenza e tutela di persone in condizioni di disagio. Interventi di assistenza e di supporto volti all'inclusione e all'integrazione sociale, lavorativa, abitativa anche di cittadini immigrati.

Le categorie di persone interessate sono:
Minori e adulti di ambo i sessi in situazione di disagio e con necessità di tutela e protezione.

I dati a carattere personale (personali) trattati sono :
dati comuni (generalità, C.F. etc.) ; dati sensibili : stato di salute, origini razziali ed etniche, dati giudiziari, biometrici, convinzioni religiose, politiche, filosofiche e di altro genere, vita sessuale;

Le operazioni eseguite sui dati sono:
raccolta, registrazione, elaborazione anche in forma cartacea e con modalità informatizzata, estrapolazione, elaborazioni statistiche semplici per monitoraggio, conservazione, comunicazione.

La categoria di destinatari della comunicazione dei dati sono:
ASUR; Strutture sanitarie pubbliche o private; Specialisti (Medici di base, Pediatri, Psicologi, Neurologi, Logopedisti etc.); Autorità Giudiziaria (Tribunali e Procure); Prefettura; Questura; Forze dell'Ordine; Centro antiviolenza Polizia Municipale; Istituti di pena; U.E.P.E.; Servizio Sociale Minorenni Min. Giustizia; Centro per l'Impiego; Enti di Formazione professionale e occupazione pubblici e privati; Agenzie autorizzate di lavoro temporaneo, Associazioni industriali e Aziende private no profit e for profit; Privato Sociale ed Enti della rete di Volontariato impegnato nell'area dii intervento; rete parentale e amicale; Soggetti gestori di strutture o di servizi esternalizzati o a titolarità privata; Agenzie immobiliari e privati proprietari di alloggi; Istituzioni scolastiche e Universitarie pubbliche e private; Servizi Educativi (Nidi, Scuole Materne); Uffici interni ed esterni anche per erogazione di servizi o agevolazioni tariffarie (es. Aziende di trasporto); Osservatori Regionale per le Politiche Sociali e/o abitative; INPS/S.I.U.S.S.; Altri Enti pubblici o privati autorizzati al trattamento per l'efficacia dell'intervento o per acquisizione/accertamento dati o a fini statistici o per altre finalità pubbliche (es. INPS; Agenzia Entrate; Agenzia del Territorio etc.).

Per l'esecuzione del servizio oggetto del presente contratto, il Titolare mette a disposizione del Responsabile del trattamento le seguenti informazioni necessarie:

- Valutazione sociale che può recare le informazioni sui dati sensibili sopra indicati, al fine di assicurare un intervento appropriato ai bisogni espressi dell'interessato.

Art. 3 - Durata del contratto
Il presente contratto ha validità per il periodo di efficacia del contratto principale cui è collegato relativo all'accoglienza di minori e/o di adulti/e, inviati/e dal Comune di Pesaro, presso una struttura autorizzata iscritta all'Elenco aperto di cui all'Avviso pubblico del 23 maggio 2018, gestita dal Responsabile del Trattamento, fino al 30 giugno 2020 o data successiva nel caso si protragga ulteriormente, la permanenza delle persone inserite in accoglienza inviate dal Comune di Pesaro, in qualità di Titolare del Trattamento

Art. 4 - Obblighi del Responsabile del trattamento di fronte al Titolare del trattamento
Il Responsabile del trattamento si impegna a:

1. Trattare i dati solo per la finalità o le finalità sopra specificate e per l'esecuzione delle prestazioni contrattuali.
2. Trattare i dati conformemente alle istruzioni del Titolare. Se il Responsabile del trattamento considera che una istruzione costituisca una violazione del regolamento europeo sulla protezione dei dati o di tutte le altre disposizioni delle leggi dell'Unione o delle leggi degli stati membri relative alla protezione dei dati, deve informare immediatamente il Titolare.
   Se il Responsabile del trattamento è tenuto a procedere ad un trasferimento dei dati verso un paese terzo o un'organizzazione internazionale, in virtù delle leggi dell'Unione o delle leggi dello stato membro al quale è sottoposto, deve informare il Titolare del trattamento di quest'obbligo giuridico prima del trattamento, a meno che le leggi interessate proibiscano una tale informazione per motivi importanti di interesse pubblico.
3. Garantire la riservatezza dei dati a carattere personale trattati nell'ambito del presente contratto.
4. Controllare che le persone autorizzate a trattare i dati personali in virtù del presente contratto:
   - si impegnino a rispettare la riservatezza o siano sottoposti ad un obbligo legale appropriato di segretezza;
   - Ricevano la formazione necessaria in materia di protezione dei dati a carattere personale.
5. Tenere conto, utilizzando i materiali, i prodotti, le applicazioni od i servizi, dei principi di protezione dei dati a partire da quando questi vengono progettati e della protezione dei dati di default.

6. Ulteriore Responsabile del trattamento
Il Responsabile del trattamento può ricorrere ad un altro Responsabile del trattamento (di seguito, "l'ulteriore Responsabile del trattamento") per gestire attività di trattamento specifiche. In questo caso, informa in precedenza e per iscritto il Titolare di ogni cambiamento riguardante l'aggiunta o la sostituzione di altri Responsabili. La predetta informazione deve indicare chiaramente le attività di trattamento delegate, l'identità e gli indirizzi dell'ulteriore Responsabile del trattamento ed i dati del contratto di esternalizzazione. Il Titolare del trattamento entro 30 giorni a partire dalla data di ricevimento dell' informazione, può presentare proprie obiezioni.
L'ulteriore Responsabile del trattamento deve rispettare gli obblighi del presente contratto per conto e secondo le istruzioni del Titolare del trattamento. Spetta al Responsabile del trattamento iniziale assicurare che l'ulteriore Responsabile del trattamento presenti le stesse garanzie sufficienti alla messa in opera di misure tecniche ed organizzative appropriate di modo che il trattamento risponda alle esigenze del Regolamento Europeo sulla protezione dei dati.
Il Responsabile del trattamento iniziale, è in ogni caso, interamente responsabile davanti al Titolare anche dell'esecuzione del trattamento da parte dell'Ulteriore Responsabile delle cui inadempienze o violazioni, risponde direttamente e personalmente.

7. Diritto di informazione delle persone interessate
Il Responsabile del trattamento, al momento della raccolta dei dati, deve fornire alle persone interessate dalle operazioni del trattamento, le informazioni relative ai trattamenti dei dati che esso realizza. La formulazione ed il formato dell'informazione deve essere convenuta con il Titolare del trattamento prima della raccolta dei dati.

8. Esercizio dei diritti delle persone
Il Responsabile del trattamento previa condivisione con il Titolare, deve rispondere, in nome e per conto del Titolare stesso e nei tempi previsti dal regolamento europeo sulla protezione dei dati, alle domande delle persone interessate qualora queste esercitino i loro diritti, dato che si tratta di dati che sono oggetto della prestazioni previste dal presente contratto.

9. Notifica della violazione di dati a carattere personale

Previo accordo con il Titolare, il Responsabile del trattamento notifica al Garante per la protezione dei dati personali, in nome e per conto del Titolare del trattamento, le violazioni di dati a carattere personale senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora detta notifica non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.

La notifica deve almeno:

a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;

b) comunicare il nome e i dati di contatto del Responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;

c) descrivere le probabili conseguenze della violazione dei dati personali;

d) descrivere le misure adottate o di cui si propone l'adozione da parte del Titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

Previo accordo con il Titolare, il Responsabile del trattamento comunica, in nome e per conto del Titolare del trattamento, la violazione di dati a carattere personale alla persona interessata al più presto, qualora tale violazione sia suscettibile di generare un rischio elevato per i diritti e le libertà di una persona fisica.

La comunicazione alla persona interessata descrive, in termini chiari e semplici, la natura della violazione di dati a carattere personale e deve contenere almeno tutte le informazioni contenute nella notifica al Garante per la protezione dei dati personali, indicate al precedente punto

10. Assistenza del Responsabile del trattamento nell'attuazione degli obblighi del Titolare del trattamento

Il Responsabile del trattamento assiste il Titolare nella realizzazione di analisi d'impatto relativa alla protezione dei dati, conformemente all'articolo 35 del Regolamento UE 206/679.

Il Responsabile del trattamento assiste il Titolare nella consultazione preventiva dell'autorità di controllo, prevista dall'articolo 36.

11. Misure di sicurezza

Il Responsabile del trattamento s'impegna a mettere in opera le misure di sicurezza tecniche ed organizzative previste nell'allegato 2 alla Determinazione del Segretario Generale n. 1276 del 24 maggio 2018 relative alle misure a protezione dei dati personali trattati nell'ambito delle funzioni istituzionali del Comune di Pesaro Titolare del Trattamento, per quanto applicabili; deve essere in ogni caso garantito *un* livello di sicurezza idoneo al rischio e devono essere garantiti, fra gli altri:

a) la pseudonimizzazione e la cifratura dei dati personali;

b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità dei sistemi e dei servizi di trattamento;

c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;

d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

12. Disposizione dei dati al termine delle prestazioni contrattuali

Il Responsabile del trattamento dovrà utilizzare i dati esclusivamente per il tempo strettamente necessario ad assicurare i percorsi di accoglienza delle persone inviate dal Comune di Pesaro e a tale fine si impegna, al momento delle dimissioni dei singoli utenti, a cessare qualunque utilizzo dei dati limitandosi a custodire e conservare con modalità che garantiscano la totale riservatezza, esclusivamente i dati che possano assumere rilevanza in caso di indagini o richieste di informazioni da parte dell'Autorità Giudiziaria, per il tempo ritenuto necessario a tale scopo e comunque per un periodo non superiore ad anni 10 (dieci). Contestualmente, il Legale Rappresentante dell''Ente gestore

trasmette apposita dichiarazione di responsabilità nella quale attesta l'impegno a rispettare la presente clausola contrattuale.

13. Responsabile della protezione dei dati

Il Responsabile del trattamento comunica al Titolare del trattamento il nome ed i dati del proprio Responsabile della protezione dei dati, qualora ne abbia designato uno conformemente all'articolo 37 del regolamento europeo sulla protezione dei dati.

14. Registro delle categorie di attività di trattamento

Il Responsabile del trattamento dichiara di tenere per iscritto un Registro di tutte le categorie di attività di trattamento effettuate per conto del Titolare del trattamento e che comprende:

- Il nome ed i dati del Titolare del trattamento per conto del quale lui tratta, del / dei Responsabile/i e, se applicabile, del Responsabile della protezione dei dati;
- Le categorie di trattamenti effettuati per conto del Titolare del trattamento;
- Se applicabili, i trasferimenti di dati a carattere personale verso un paese terzo o ad una organizzazione internazionale e, nel caso di trasferimenti previsti dall'articolo 49, paragrafo 1, secondo comma del Regolamento Europeo sulla Protezione dei dati, i documenti che attestano l'esistenza di opportune garanzie;
- Per quanto possibile, una descrizione generale delle misure di sicurezza tecniche ed organizzative, ivi compresi, fra gli altri, secondo le necessità:
    - La pseudonimizzazione e la numerazione dei dati a carattere personale;
    - I mezzi che permettono di garantire la segretezza, l'integrità, la disponibilità e la resilienza costanti dei sistemi e dei servizi di trattamento;
    - I mezzi che permettono di ristabilire la disponibilità dei dati a carattere personale e l'accesso a questi nei tempi appropriati in caso di incidente fisico o tecnico;
    - Una procedura che mira a testare, ad analizzare ed a valutare regolarmente l'efficacia delle misure tecniche ed organizzative per assicurare la sicurezza del trattamento.

15. Documentazione

Il Responsabile del trattamento mette a disposizione del Titolare la documentazione necessaria per dimostrare il rispetto di tutti gli obblighi e per permettere la realizzazione di revisioni, comprese le ispezioni, da parte del Titolare o di un altro revisore che questi abbia incaricato, e contribuire a queste revisioni.

Art. 5 Obblighi del Titolare del trattamento di fronte al Responsabile del trattamento

Il Titolare del trattamento s'impegna a:

- Comunicare le modifiche alle Misure di sicurezza adottate dal Titolare per quanto applicabili al Responsabile del trattamento da intendersi quali Misure minime; il Responsabile del Trattamento deve comunque essere dotato di un proprio Sistema di protezione dei dati personali tale da garantire livelli adeguati di sicurezza a tutela degli interessati;
- Vigilare, in anticipo e durante la durata di tutto il trattamento, sul rispetto degli obblighi previsti dal regolamento europeo sulla protezione dei dati da parte del Responsabile del trattamento.

Art. 6 Misure Tecniche ed organizzative

Ai sensi e per gli effetti di cui al precedente articolo 4, comma 11, si riporta di seguito l'allegato 2 alla Determinazione del Segretario Generale del Comune di Pesaro n. 1276 del 24 maggio 2018 relativo alle misure di sicurezza tecniche ed organizzative che il Responsabile del Trattamento si impegna a mettere in opera:

MISURE TECNICHE E ORGANIZZATIVE A PROTEZIONE DEI DATI PERSONALI TRATTATI NELL'AMBITO DELLE FUNZIONI ISTITUZIONALI DEL COMUNE DI PESARO

A) PREMESSA E MISURE GENERALI DA OSSERVARE CON RIFERIMENTO A TUTTE LE TIPOLOGIE DI DATI

Il **diritto alla riservatezza ed alla protezione dei propri dati personali** è principio che deriva direttamente dalla Carta Costituzionale e costituisce un diritto della personalità. Il rispetto di tale diritto da parte di tutti gli operatori autorizzati del Comune di Pesaro, corrisponde ad una precisa **scelta di qualità nei rapporti con i propri cittadini – utenti**. Pertanto ogni Operatore autorizzato al trattamento di dati personali è tenuto a:

- rispettare le regole per il corretto e sicuro trattamento dei dati e per l'utilizzo degli strumenti informatici;
- rispettare le ulteriori Disposizioni, verbali o scritte, finalizzate alla sicurezza degli archivi cartacei ed informatici fornite dal Responsabile del Servizio;
- informare immediatamente e collaborare con il Responsabile del Servizio in merito ad ogni questione rilevante ai fini della applicazione della normativa in oggetto relazionando in merito agli adempimenti ritenuti opportuni sulle singole procedure suggerendo disposizioni operative ed accorgimenti per la sicurezza delle banche dati e dei procedimenti di gestione e/o trattamento delle stesse.

B) OBBLIGHI DI SICUREZZA DEI DATI

I dati devono essere trattati in modo tale da **prevenire e ridurre al minimo, mediante idonee misure di sicurezza e attraverso precise modalità comportamentali**, i rischi di **distruzione**, **perdita** anche accidentale, **accesso non autorizzato**, **trattamento non consentito o non conforme agli scopi della raccolta**. Pertanto ogni Operatore autorizzato al trattamento, è tenuto ad osservare le seguenti misure di sicurezza:

B1.) Banche dati gestite in formato elettronico: valutazione del rischio e principali misure tecnico-organizzative.

L'art 32 del Regolamento UE/2016/679 tratta i principi che riguardano la 'Sicurezza del trattamento', in questo documento si vogliono evidenziare i principali aspetti riguardanti la sicurezza del trattamento analizzandone i rischi presentati dal trattamento stesso e le misure tecniche e organizzative che si ritiene di dover adottare per mitigare tali 'rischi'.

Gli aspetti principali che riguardano la sicurezza di un trattamento derivano dai seguenti criteri da preservare quando si parla di dati personali:

- Disponibilità
- Integrità
- Riservatezza

In relazione a questi criteri, i principali rischi inerenti il trattamento dei dati sono:

- rischio di **distruzione** accidentale o illegale
- rischio di **perdita** dei dati
- rischio di **indisponibilità** dei dati
- rischio di **alterazione** non voluta
- rischio di **comunicazione** e **diffusione** non consentita
- rischio di **accesso** non autorizzato

Nel valutare un adeguato livello di sicurezza per il trattamento si tiene conto del fatto che i rischi derivano dal verificarsi di eventi relativi al comportamento degli operatori, eventi relativi agli strumenti utilizzati, eventi relativi al contesto fisico-ambientale quali ad esempio:

1) eventi relativi al comportamento degli operatori:
- sottrazione di credenziali di autenticazione
- carenza di consapevolezza, disattenzione o incuria
- comportamenti sleali o fraudolenti
- errore materiale

2) eventi relativi agli strumenti:
- azione di virus informatici o di programmi suscettibili di recare danno
- spamming o tecniche di sabotaggio

- malfunzionamento, indisponibilità o degrado degli strumenti
- accessi esterni non autorizzati
- intercettazione di informazioni in rete

3) eventi relativi al contesto fisico-ambientale:
- ingressi non autorizzati a locali/aree ad accesso ristretto
- sottrazione di strumenti contenenti dati
- eventi distruttivi, naturali o artificiali (movimenti tellurici, scariche atmosferiche, incendi, allagamenti, condizioni ambientali, ecc.), nonché dolosi, accidentali o dovuti ad incuria
- guasto a sistemi complementari (impianto elettrico, climatizzazione, ecc.)
- errori umani nella gestione della sicurezza fisica

Tutto ciò premesso dall'analisi dei rischi e degli eventi da cui essi derivano si individuano le principali misure tecniche organizzative utili al fine di garantire un livello di sicurezza adeguato al rischio.

1) Istruzione e formazione del personale:
- informativa sulla custodia e rinnovo frequente delle credenziali di autenticazione
- formazione puntuale sull'utilizzo degli applicativi gestionali
- sensibilizzazione del personale
- informativa sui possibili attacchi virali provenienti dalla rete
- vigilanza dei responsabili dei trattamenti

2) Sicurezza logica relativa agli strumenti tecnologici utilizzati:
- sistema di identificazione, autenticazione e autorizzazione degli utenti
- gestione dei diritti di accesso ai servizi applicativi con i privilegi minimi necessari all'utente
- unico sistema di *repository* delle credenziali di accesso degli utenti ad uso di alcuni applicativi
- Log degli accessi e delle operazioni sui vari applicativi
- log di sistema, generati dal sistema operativo
- log dei dispositivi di protezione periferica del sistema informatico
- utilizzo di cartelle per la condivisione di documenti di lavoro su server accessibili via rete
- applicazione di tecniche di cifrature o pseudonimizzazione nel caso di dati personali più sensibili
- sistema di aggiornamento e patching dei sistemi server e client
- utilizzo di protocolli di trasmissione sicuri (https, ssh,…)
- utilizzo di procedure di backup centralizzate e automatizzate
- utilizzo di firewall e filtri sulla navigazione Internet
- utilizzo di programmi antintrusione
- utilizzo di programmi antispam
- utilizzo di un sistema antivirus centralizzato e monitorato
- utilizzo di configurazioni sicure e standard nella predisposizione delle postazioni di lavoro
- verifica periodica degli strumenti e loro sostituzione

3) Sicurezza relativa al contesto fisico-ambientale:
- utilizzo di sistemi Cloud Microsoft (Office365 e Azure) compliance con il GDPR
- nel Datacenter sono disponibili i seguenti impianti, atti a garantire la sicurezza fisica dei dati:
  - allarme antincendio
  - controllo degli accessi e dei varchi fisici
  - gruppo di continuità (UPS) dimensionato
  - climatizzazione degli ambienti
  - sistemi di allarme antintrusione e antincendio
  - verifica periodica degli strumenti e manutenzione programmata

Le suddette misure verranno dettagliate in fase operativa, in collaborazione con il Responsabile dei Sistemi Informativi del Comune.

B2.) Misure volte a prevenire in particolare, il rischio di perdita (anche accidentale) e/o distruzione dei dati:

- I documenti cartacei contenenti dati personali non possono essere portati al di fuori dei locali già individuati ed utilizzati per la loro conservazione se non per necessità istituzionali e per il tempo strettamente necessario ai relativi scopi; in tale caso l'incaricato non dovrà mai lasciare incustoditi i documenti assicurandosi altresì che gli stessi siano completi ed integri soprattutto quando composti di numerose pagine o di allegati;
- a fine giornata di lavoro, gli incaricati al trattamento dei dati devono provvedere:
  - a riporre tutti i documenti contenenti dati personali in contenitori, cassetti, armadi dotati di chiave;
  - alla chiusura a chiave di tutti i cassetti, contenitori, armadi etc. che custodiscono archivi di dati personali;
  - a riporre tutte le chiavi in luogo sicuro e non accessibile a sua volta chiuso a chiave (quest'ultima chiave deve essere conservata direttamente a cura dell'operatore autorizzato all'accesso alle specifiche banche dati);
  - allo spegnimento della luce dell'ufficio nonché allo spegnimento degli elaboratori togliendo completamente corrente dalla apposita ciabatta elettrica al fine di non incorrere in rischi di distruzione di archivi per possibili corti circuiti o rischi incendi per surriscaldamento della macchina.

B3.) Misure volte a prevenire il rischio di accessi non autorizzati:

B3.1.) Modalità di conservazione dei dati:

- adottare ogni cautela onde evitare che soggetti non autorizzati possano anche casualmente, venire a conoscenza di dati personali;
- quando l'Operatore autorizzato al trattamento si debba allontanare temporaneamente dalla propria stanza in assenza di altri operatori che possano controllare l'accesso da parte di soggetti terzi, deve bloccare il proprio computer utilizzando contemporaneamente i tasti *Alt+Ctrl+Canc* e cliccando poi su *"Blocca computer"* al fine di richiedere la password per un nuovo accesso; nel caso in cui vi siano documenti cartacei incustoditi deve provvedere chiudendo a chiave la stanza;
- nella gestione delle chiavi di armadi e porte dei locali, ogni Operatore deve rispettare le istruzioni di cui al precedente paragrafo B2) ;
- quando documenti contenenti dati sensibili debbano essere portati al di fuori della sede presso la quale sono conservati o presso la quale sono stati prodotti (es. trasferimento all'ufficio Protocollo), l'Operatore avrà cura di tenere con sé la cartella che li contiene evitando che terzi possano visionare anche solo la copertina del fascicolo;
- evitare in qualunque momento il deposito di atti o documenti contenenti dati personali, anche registrati su supporto magnetico mobile, quando ciò sia espressamente autorizzato, in luoghi accessibili a chiunque (scrivanie, fotocopiatrici, stampanti, fax……), al fine di impedire accessi non autorizzati sia in orario di servizio sia durante la chiusura al pubblico;
- conservare in armadi e/o contenitori chiusi a chiave, tutti i documenti cartacei e/o, cd, dvd, pennetta se autorizzato l'uso di supporto magnetico mobile, che contengano dati personali;
- evitare per quanto possibile, la duplicazione di archivi anche limitando l'uso delle copie fotostatiche allo stretto indispensabile;
- è vietato l'uso di copie fotostatiche non utilizzate o comunque di atti e documenti recanti dati personali come carta per appunti a meno che non venga comunque conservata in contenitori chiusi a chiave prima dell'utilizzo per poi essere distrutta;
- è vietato gettare nel cestino o nel contenitore per carta da riciclare, atti e documenti contenenti dati sensibili non previamente distrutti, in modo tale da renderli inintelleggibili;
- eliminare i "brogliacci" contenenti dati sensibili, giudiziari o comunque riservati, utilizzati per la definizione di pratiche, che non costituiscano documento da conservare, attraverso l'apposita "distruggidocumenti" *(in carenza di attrezzatura distruggidocumenti, si dovrà provvedere a distruggere i brogliacci in modo tale da assicurare la loro totale illeggibilità).*

B4.) Altre misure fisiche di custodia dei dati:

B4.1.) Accesso agli <u>archivi cartacei controllati (contenenti dati sensibili, giudiziari o di particolare natura) ubicati presso i singoli uffici</u>:

I dati necessari per lo svolgimento dei compiti lavorativi propri di ciascun Operatore autorizzato al trattamento, sono custoditi in armadi muniti di serratura e debitamente chiusi a chiave a cura del/dei dipendente/i che occupa/occupano l'ufficio designato/i formalmente incaricato/i della custodia degli archivio/i ad accesso controllato. L'accesso a tali banche dati pur di utilizzo quotidiano, è selezionato per cui deve avvenire, da parte degli stessi Operatori autorizzati, esclusivamente nei limiti in cui ciò sia strettamente necessario per prelevare e riporre i documenti (e/o i supporti informatici rimovibili quando dovesse esserne autorizzato l'uso) necessari per lo svolgimento delle specifiche funzioni. Durante l'utilizzo, i documenti dovranno essere vigilati e custoditi in maniera che ad essi non accedano persone prive di autorizzazione. Durante i periodi di temporanea assenza ed al termine della giornata lavorativa, i documenti prelevati dovranno essere riposti in cassetti/contenitori chiusi a chiave. Una volta terminato il lavoro per svolgere il quale si è reso necessario utilizzare i documenti, essi dovranno essere ricollocati nell'archivio dal quale sono stati prelevati e chiusi a chiave.

B4.2.) Accesso ad archivi controllati, di deposito o non ubicati presso uffici specifici (contenenti dati sensibili, giudiziari o di particolare natura):
L'accesso a banche dati contenenti dati sensibili, di natura giudiziaria o di particolare natura, conservate presso archivi di deposito, è controllato, per cui ciascun Operatore o qualunque altra persona ammessa a qualunque titolo, può accedervi anche durante l'orario di lavoro, solo previa autorizzazione del Responsabile delle chiavi individuato dal Dirigente di Servizio. In carenza di nomina del Responsabile della custodia per l'accesso agli archivi, è necessario rivolgersi al Dirigente del Servizio.

L'accesso al di fuori dell'orario lavorativo, dovrà essere autorizzato direttamente dal Dirigente del Servizio.

B4.3.) Gestione chiavi ufficio
Le chiavi delle porte dei singoli uffici non devono essere mai tenute sulle porte (in particolare all'esterno dell'ufficio), per motivi di sicurezza. Dette chiavi devono essere utilizzate nel caso in cui il dipendente esca dagli uffici del Servizio in assenza di colleghi, durante la giornata di lavoro e per altre assenze (ad es. pausa pasto).

C) TRASMISSIONE DI DATI SENSIBILI, GIUDIZIARI O DI PARTICOLARE NATURA, ALL'INTERNO DELL'ENTE

C1) Comunicare, i dati sensibili e giudiziari ad altri servizi dell'Ente autorizzati al trattamento, nel rispetto della riservatezza, procedendo ad inserire il documento o la certificazione in busta chiusa recante all'esterno la dicitura "contiene dati sensibili – da aprire solo a cura del destinatario"; qualora venga utilizzato il fax, accertarsi preventivamente che l'operatore dell'ufficio ricevente proceda a prelevarlo con immediatezza onde evitare accessi non autorizzati;

C2) Controllare e monitorare l'andamento dei flussi informativi e delle relative modalità di comunicazione di dati sensibili o giudiziari o comunque, di particolare natura, con gli altri servizi dell'Ente eliminando i comportamenti scorretti, riferendo al Responsabile del Servizio, eventuali anomalie riscontrate e suggerendo gli opportuni accorgimenti;

D) USO DEGLI STRUMENTI DEL TRATTAMENTO

D1. Telefono:

- è vietato discutere, comunicare o comunque trattare dati personali per telefono se non si è assolutamente certi che il destinatario sia un operatore autorizzato a trattare i dati in questione;
- in ogni caso, non possono essere forniti dati sensibili, giudiziari o particolari, via telefono a soggetti privati.
- nel caso di richieste di informazioni via telefono da parte di organi di amministrazioni pubbliche, A.S.U.R.- Zona Territoriale, forze di P.S., Autorità Giudiziarie, etc. può essere necessario, quando non si abbia la certezza che il chiamante sia un soggetto autorizzato al trattamento dei dati, procedere nel seguente modo:
  - chiedere ed accertare l'identità del chiamante e la motivazione della richiesta;

- verificare a chi corrisponde il telefono chiamante differendo il riscontro della richiesta, se pure nel rispetto dei principi di celerità ed efficienza;
- procedere immediatamente a richiamare la persona che ha richiesto le informazioni, con ciò accertandosi della identità dichiarata in precedenza;

- non parlare mai ad alta voce, trattando dati personali per telefono, per evitare che i dati possano essere conosciuti da terzi non autorizzati, anche accidentalmente; tale modalità va scrupolosamente osservata quando il telefono è ubicato in luogo aperto al pubblico.

D2.) Utilizzo posta elettronica e fax: occorre inserire, in calce alla comunicazione, la seguente dicitura:

"Il testo e gli eventuali documenti trasmessi contengono informazioni riservate esclusivamente al/ai destinatario/i indicato/i. Il contenuto della presente e-mail /fax e dei suoi eventuali allegati, è confidenziale e la sua riservatezza è tutelata legalmente dalla vigente normativa in materia di riservatezza. La lettura, utilizzo, comunicazione, diffusione copia o altro uso non autorizzato o qualsiasi altra azione derivante dalla conoscenza di queste informazioni sono rigorosamente vietate e sanzionate dall'ordinamento. **Qualora abbiate ricevuto questo documento per errore, siete cortesemente pregati di darne immediata comunicazione al mittente ai numeri qui indicati (tel. 0721/387…..) e/o all'indirizzo dello stesso e di provvedere immediatamente alla distruzione del contenuto** *della presente e-mail/fax. This message and its attachments are addressed solely to the persons above and may contain confidential information. If you have received the message in error, be informed that any use of the content hereof is prohibited. Please return it immediately to the sender and delete the message."*

D3.) Fotocopiatrice e scanner:

- la stampa e la scansione dei dati deve essere effettuata solo se strettamente necessario. La fotocopia deve essere ritirata prontamente dai vassoi della stampante;
- nella duplicazione di documentazione (con stampanti o fotocopiatrici o altre periferiche) si deve fare attenzione a non lasciare originale e/o copie incustodite;
- in caso di inceppamento, i fogli non utilizzabili recanti dati personali dovranno essere distrutti evitando di gettare la documentazione nel cestino o nel contenitore della carta straccia senza aver previamente provveduto a rendere inintelligibile il contenuto anche con l'apparecchio distruggi documenti.

E) Utilizzo della posta elettronica e accesso a Internet: si rinvia alle modalità previste dalle Misure di sicurezza dei trattamenti informatizzati predisposto dal Responsabile del Servizio Sistemi Informativi.

F) Policy di accesso al sistema informativo dell'ente

Verrà fornita a ciascun dipendente, l'autorizzazione per accedere ai dati assegnando un profilo di accesso.

Tutto quanto non espressamente autorizzato dal Dirigente Servizio, è da intendersi come vietato.

Tutti i dati inclusi quelli comuni dovranno essere utilizzati nei limiti strettamente necessari per lo svolgimento della attività lavorativa, mantenendo il massimo riserbo come previsto dalla vigente normativa in materia di riservatezza.

G) Comunicazione di dati personali comuni a soggetti pubblici e privati
La comunicazione di dati personali comuni a soggetti pubblici e a soggetti privati può essere effettuata solo quando sia prevista da apposita norma di legge o di regolamento.
In merito, il Comune di Pesaro con fonte secondaria (Regolamento approvato con delibera di Consiglio Comunale n. 19 del 12.3.2007 – art. 8) ha disciplinato, ad integrazione delle fonti primarie, la possibilità di comunicazione a soggetti pubblici o privati o la diffusione di dati personali comuni, purché la comunicazione o la diffusione, risponda ad una delle seguenti finalità già perseguite dall'Ente:

a. Finalità nell'ambito delle attività di amministrazione generale e contabilità;
b. Finalità di accertamento e riscossione di tasse ed imposte;
c. Finalità nell'ambito di attività istituzionali in ambito comunitario e/o internazionale (accordi di collaborazione e gemellaggio);
d. Finalità nell'ambito delle attività di servizi informativi e di relazioni con il pubblico;
e. Finalità nell'ambito della promozione e diffusione di attività culturali, sportive, turistiche, ricreative e di valorizzazione del tempo libero;
f. Finalità nell'ambito delle attività di educazione e istruzione;
g. Finalità in ambito sociale, socio – assistenziale, socio-educativo;
h. Finalità nell'ambito delle attività di promozione economica del territorio;
i. Finalità di promozione e diffusione dell'Associazionismo, dei valori di solidarietà e di valorizzazione della sussidiarietà e delle iniziative spontanee della società civile;
j. Finalità di difesa dell'ambiente e della sicurezza della popolazione;
k. Finalità di pianificazione urbanistica e amministrazione del territorio;
l. Finalità di progettazione, affidamento o esecuzione di opere pubbliche;
m. Finalità di protezione civile.

In presenza di richiesta di accesso agli atti, anche sotto forma di mera consultazione, gli Operatori dovranno sempre e comunque fare riferimento al Dirigente del Servizio.
E' vietata la comunicazione o la diffusione di dati al di fuori di quanto sopra indicato.

H) Comunicazione di dati a soggetti terzi o comunque con strumenti impersonali o che non consentono un controllo effettivo dell'identità del chiamante. La comunicazione va effettuata con particolare attenzione a:

- **controllo dell'identità del richiedente:** nel caso di richieste di comunicazione di dati (presentate per telefono o per fax) occorre verificare l'identità del soggetto richiedente;
- **verifica dell'esattezza dei dati comunicati:** nell'accogliere una richiesta di comunicazione di dati personali, da parte dell'interessato ovvero di un terzo a ciò delegato, occorre fare attenzione all'esattezza del dato che viene comunicato, in particolare quando la richiesta viene soddisfatta telefonicamente o attraverso trascrizione da parte dell'operatore, di quanto visualizzato sul monitor.

I) Operatori addetti al pubblico, rapporti di front-office. Nei servizi di relazione con il pubblico dovrà essere prestata attenzione a:

- rispetto della **distanza di sicurezza**: gli operatori di uffici aperti al pubblico devono prestare attenzione al rispetto dello spazio di cortesia e se del caso invitare gli utenti ad accomodarsi fuori dell'ufficio attendendo il proprio turno;
- **identificazione dell'interessato:** in alcuni casi può essere necessario dover identificare il soggetto interessato per esigenze di garanzia di correttezza del dato da raccogliere (si pensi a soggetti stranieri ovvero a dati identificativi che possono generare dubbi sulla correttezza della registrazione) ovvero con riferimento alla personalità della prestazione richiesta: può essere necessario richiedere ed ottenere un documento di identità o di riconoscimento ove si abbia un dubbio sulle modalità di scrittura del nome e cognome dell'interessato o si voglia avere garanzia dell'effettiva identità del soggetto interessato;
- **controllo dell'esattezza del dato:** fare attenzione alla digitazione ed all'inserimento dei dati identificativi dell'interessato, al fine di evitare errori di battitura ed assicurare la correttezza del dato.

L) Trattamenti di dati sensibili e di natura giudiziaria
Il trattamento di dati sensibili e giudiziari è consentito nelle modalità e nei termini specificati in apposito atto regolamentare.

M) Obbligo di riservatezza e segretezza:
L'Incaricato del trattamento deve mantenere l'assoluta segretezza sulle informazioni di cui venga a conoscenza nel corso delle operazioni del trattamento e deve evitare qualunque comunicazione / diffusione non espressamente autorizzata da fonte normativa. L'eventuale violazione dell'obbligo ivi considerato può comportare l'applicazione di sanzioni di natura disciplinare ed una responsabilità civile e penale, secondo quanto previsto dalla vigente normativa.

Per il Titolare del Trattamento
Comune di Pesaro

Per il Responsabile del Trattamento
Impresa / Professionista

U.O. Gestione Attività Servizio Sociale Prof.le
d.ssa Carla Romanello

…… ……