SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA
Azienda Unità Sanitaria Locale di Parma

ATTO DI DESIGNAZIONE
DI SOGGETTO AUTORIZZATO AL TRATTAMENTO DEI DATI PERSONALI

L'Azienda USL di Parma, in qualità di Titolare del trattamento dei dati personali, nella persona del Delegato del trattamento **Dott. Alberto Grazioli, Responsabile Aziendale dei tirocini in psicologia – psicoterapia**, ai sensi e per gli effetti di cui agli artt. 29 e 32, par. 4, del Regolamento (UE) 2016/679 e 2-quaterdecies del D. Lgs. 30 giugno 2003, n. 196

AUTORIZZA

Il Sig./La Sig.ra _____ c.f. _____, (di seguito, "autorizzato"), nella sua qualità di TIROCINANTE, ad eseguire operazioni di trattamento di dati personali *necessari*, *non eccedenti* e *pertinenti* allo svolgimento delle attività di formazione e orientamento in ambito psicologico, consistenti in:

- Accesso a dati clinici
- Osservazione colloqui psicologici
- Interpretazione reattivi psicodiagnostici
- Stesura relazioni cliniche
- Equipe multiprofessionali di natura clnica o psico-sociale
- ……..
- ……..

Le operazioni di trattamento devono essere limitate a quanto necessario e indispensabile all'adempimento delle suddette attività, osservando le norme di legge, le politiche, i regolamenti e le procedure aziendali nonché le istruzioni impartite dal Titolare del trattamento, dal suo Delegato e/o dal Responsabile della Protezione dei Dati.

L'autorizzato è tenuto ad eseguire le operazioni di trattamento nel pieno rispetto dei diritti, delle libertà fondamentali e della dignità degli interessati, in modo lecito e sicuro, verificando, ove possibile, che i dati siano adeguati, pertinenti, completi, esatti ed aggiornati. Per quanto riguarda i dati relativi alla salute, deve attenersi al segreto professionale e ad ogni altro obbligo di segretezza, incluso il segreto d'ufficio, mantenendo riservate le informazioni *anche al termine* del tirocinio.

È fatto assoluto divieto di trattare dati per finalità estranee alle attività di cui alla presente autorizzazione.

Ogni attività di trattamento di dati effettuata attraverso modalità elettroniche è registrata attraverso apposito *file log* conservati per il tempo necessario a dare riscontro ad eventuali istanze relative all'esercizio dei diritti da parte degli interessati e per eventuali attività di *audit*. In caso di incidenti di sicurezza che comportino la violazione di dati (es. distruzione, perdita, modifica, indisponibilità anche temporanea, divulgazione non autorizzata o accesso illecito ai dati personali trattati), l'autorizzato è tenuto a farne tempestiva segnalazione al Delegato del trattamento (il Responsabile dell'UO di afferenza), al fine di consentire di attivare le procedure previste per annullare o ridurre l'impatto della violazione sui diritti e libertà degli interessati, secondo quanto previsto dalla procedura aziendale di gestione dei casi di *data breach*.

L'autorizzato è tenuto a tenersi informato ed aggiornato circa le istruzioni, informazioni ed indicazioni rese dal Titolare o dal suo Delegato al trattamento.

La presente designazione ha efficacia per tutto il tempo in cui è svolta l'attività di tirocinio. Potrà essere oggetto di modifica o integrazione in relazione alle attività formative demandate, alle peculiarità e specificità dei compiti assegnati e dei relativi trattamenti da eseguire.

Luogo e data, _____

Il Delegato del trattamento

Alberto Grazioli

_____

L'Autorizzato

_____
per presa visione e consegna

IN ALLEGATO: ISTRUZIONI OPERATIVE

ISTRUZIONI OPERATIVE

PREMESSA

Il presente documento contiene le istruzioni operative per i soggetti autorizzati ad eseguire operazioni di trattamento dei dati personali necessari, pertinenti e non eccedenti allo svolgimento dell'attività lavorativa o di collaborazione a qualunque titolo, anche di tirocinio o formazione (di seguito "attività lavorativa"). Le presenti istruzioni possono essere oggetto di modifica ed integrazioni in relazione alle peculiarità delle operazioni di trattamento effettivamente svolte e sono dettate per prevenire condotte che, anche inconsapevolmente, possano comportare rischi per i diritti e le libertà degli interessati e per la sicurezza del sistema informativo aziendale.

DEFINIZIONI

«Dato personale»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.
«Categorie particolari di dati»: dati che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, dati genetici, dati biometrici, dati relativi alla salute, alla vita sessuale o all'orientamento sessuale.
«Dati relativi alla salute»: dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute.
«Trattamento»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.
«Titolare del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento.
«Delegato al trattamento»: persona fisica espressamente designata, interna all'organizzazione, che sotto l'autorità del titolare svolge specifici compiti e funzioni connessi al trattamento dei dati (generalmente, il Responsabile della Struttura Complessa di afferenza o Semplice Dipartimentale).
«Autorizzato al trattamento»: persona fisica, espressamente designata, che sotto l'autorità del titolare ed il controllo del delegato svolge specifici compiti e funzioni connessi al trattamento dei dati necessari allo svolgimento dell'attività lavorativa (dipendente o collaboratore a qualunque titolo).
«Responsabile del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo, che tratta dati personali per conto del titolare del trattamento (soggetto esterno all'organizzazione).
«Violazione dei dati personali»: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

PRESCRIZIONI

È vietata ogni operazione di trattamento per finalità personali o comunque diverse da quelle connesse all'attività lavorativa. Di conseguenza, possono essere trattati solo i dati strettamente necessari, pertinenti e non eccedenti al perseguimento delle finalità per le quali sono conferiti o acquisiti.
È vietato modificare i trattamenti esistenti o eseguire nuovi ed ulteriori trattamenti senza preventiva autorizzazione.
Le operazioni di trattamento autorizzate devono essere eseguite nel pieno rispetto dei principi, delle norme e delle indicazioni contenute nel Regolamento (UE) 2016/679, nel D. Lgs. 30 giugno 2003, n. 196 e nei provvedimenti del Garante per la Protezione dei Dati Personali, nonché nei regolamenti e procedure aziendali. In particolare, i trattamenti devono essere eseguiti in rispetto dei diritti, libertà fondamentali e dignità degli interessati, sotto obbligo di riservatezza e segretezza, sia professionale che d'ufficio. In particolare, è vietato rendere pubblico o comunicare con qualunque mezzo, compresi il web, social network, blog, forum e sistemi di messaggistica, commenti, informazioni, foto, video, audio che possano ledere la riservatezza e la dignità delle persone, in particolare dei pazienti, l'immagine dell'Azienda e l'onorabilità dei colleghi, o acquisire tali dati ed informazioni con dispositivi personali come ad esempio telefoni cellulari, smartphone, memorie USB, personal computer.
I dati devono essere trattati in modo lecito e sicuro previa verifica, ove possibile, che siano adeguati, pertinenti, completi, esatti ed aggiornati, avendo cura, in fase di acquisizione, di identificare opportunamente l'interessato o il soggetto che fornisce le informazioni e di registrarli ponendo particolare attenzione al momento della digitazione.
In caso di incidenti di sicurezza che comportino la violazione di dati, cd. data breach (es. distruzione, perdita, modifica, indisponibilità anche temporanea, divulgazione non autorizzata o accesso illecito ai dati personali trattati), farne tempestiva segnalazione al Delegato al fine di consentire di attivare le procedure previste per annullare o ridurre l'impatto della violazione sui diritti e libertà degli interessati.
Se non specificamente autorizzato dall'interessato, non fornire per telefono informazioni personali, in particolare quelle relative allo stato di salute, avendo cura di effettuare le eventuali comunicazioni in modalità riservata.
Nel caso in cui l'attività lavorativa preveda il contatto col pubblico, far rispettare le appropriate distanze di cortesia e, sia per l'erogazione delle prestazioni sanitarie che amministrative, avere cura di chiamare l'utente secondo riservatezza (es. mediante l'utilizzo di dispositivi regolacode).

TRATTAMENTI CON L'AUSILIO DI STRUMENTI ELETTRONICI

I dispositivi informatici e tecnologici messi a disposizione dell'Azienda devono essere utilizzati esclusivamente per lo svolgimento dell'attività lavorativa e, pertanto, non possono essere utilizzati per scopi personali. Salvo diverse ed ulteriori istruzioni ed accorgimenti, si indicano le principali misure tecniche ed organizzative ritenute necessarie per una corretta gestione degli strumenti ed applicativi informatici in dotazione.

Gestione degli strumenti elettronici

Il lavoratore/collaboratore è responsabile del corretto utilizzo e della custodia degli strumenti elettronici aziendali dati in uso per lo svolgimento delle attività, prestando particolare riguardo ed attenzione alla segretezza delle credenziali di accesso agli stessi ed ai sistemi e programmi informatici, inclusa la casella di posta elettronica, attraverso l'adozione di password rispettose dei requisiti di complessità e sicurezza raccomandati. Deve assolutamente essere impedito l'accesso ai dati ivi contenuti da parte di altri soggetti.

Per una corretta gestione delle sessioni di lavoro è necessario:

- non lasciare accessibile il *computer* in caso di momentanea assenza dalla postazione di lavoro; in caso di allontanamento, anche temporaneo, accertarsi che non vi sia possibilità da parte di terzi, anche colleghi, di accedere a dati personali per i quali sia in corso un qualunque tipo di trattamento, eseguendo il *log out* dagli applicativi o programmi informatici eventualmente in

uso e, in caso di assenza prolungata, attivare il salvaschermo (*screen saver*) protetto da credenziali di autenticazione e con avvio automatico non oltre 10 minuti dall'inattività o, in alternativa, spegnere il *computer*;

- non lasciare accessibile e/o incustodito il *computer* portatile in dotazione, avendo cura di custodirlo in armadio chiuso a chiave e rimuovere gli eventuali *file* elaborati prima della riconsegna;
- in caso di stampa di documenti contenente dati personali, in particolare attraverso una stampante condivisa, ritirare tempestivamente i documenti stampati per evitare l'accesso a soggetti non autorizzati a quel trattamento;
- al termine della giornata lavorativa, spegnere il *computer* e chiudere le parte dell'ufficio a chiave.

Anomalie o malfunzionamenti degli strumenti elettronici devono essere segnalati al Servizio Risorse Informatiche e Telematiche. Gestione username e password. L'accesso al computer di lavoro è protetto da un sistema di autenticazione che richiede l'inserimento di un codice utente (username) ed una parola chiave (password), strettamente personali e riconducibili in modo univoco all'utente utilizzatore.
Le credenziali di accesso ai programmi ed applicativi informatici sono rilasciate dal servizio RIT previa esplicita richiesta da parte del responsabile della Struttura/U.O./Ufficio di afferenza del lavoratore, devono essere scrupolosamente conservate e non devono essere rivelate o condivise con altri soggetti. Si raccomanda di non ricorrere alla funzione di salvataggio automatico delle credenziali volta a facilitare i successivi accessi.
La password deve essere scelta nel rispetto dei seguenti criteri: deve essere lunghe almeno otto caratteri; non deve fare riferimento ad informazioni agevolmente riconducibili ai soggetti utilizzatori; deve possibilmente contenere una combinazione di numeri e/o segni speciali, lettere, maiuscole e minuscole; non deve essere uguale alla precedente scaduta.

Gestione posta elettronica aziendale

Il servizio di posta elettronica deve essere utilizzato per le sole finalità lavorative.
Al fine di non compromettere la sicurezza informatica e la disponibilità dei dati, procedere all'immediata eliminazione di e-mail ricevute da destinatari sconosciuti quando vi sia il sospetto di iniziative malevoli, evitando di aprire gli eventuali allegati.
Nell'ipotesi eccezionale in cui l'e-mail debba essere utilizzata per la trasmissione di dati particolari e sensibili, si raccomanda di prestare attenzione a che l'indirizzo del destinatario sia stato correttamente digitato, che l'oggetto del messaggio non contenga direttamente informazioni idonee ad identificare l'interessato e a rivelare lo stato di salute.

Installazione di *hardware* e *software*

L'installazione di hardware e software, nonché la modifica dei parametri di configurazione del computer, possono essere eseguiti solamente dal personale tecnico del Servizio RIT. Pertanto gli utenti dei computer aziendali non sono autorizzati ad:

- utilizzare dispositivi personali, o comunque non aziendali, quali lettori, dispositivi di memorizzazione dei dati, ecc.;
- installare sistemi per connessione esterne, quali modem, wi-fi, ecc. (tali connessioni, aggirando i sistemi preposti alla sicurezza della rete aziendale, aumentano sensibilmente i rischi di intrusioni e di attacchi dall'esterno);
- installare programmi, anche in versione demo. In particolare, è vietata l'installazione di giochi, programmi in prova (shareware), programmi gratuiti (freeware), programmi pirata e, in generale, tutti i software non autorizzati;

La condivisione di aree e di risorse del computer è, in via generale, vietata. Se autorizzata dal proprio responsabile, può essere eseguita dal Servizio RIT solo in casi eccezionali e solo per il tempo strettamente necessario allo svolgimento delle attività.

Gestione dei supporti rimovibili

I supporti rimovibili di archiviazione, come ad esempio hard disk esterni, chiavette USB o CD riscrivibili, qualora contengano in via eccezionale dati personali, soprattutto sensibili, devono essere custoditi in luogo protetto e non accessibile (cassaforte, armadio chiuso a chiave, ecc.). Quando non più utilizzati, devono essere trattati in modo da non poter più recuperare i dati precedentemente memorizzati (formattazione, distruzione, ecc.).

Gestione protezione dai virus informatici

Per prevenire eventuali danneggiamenti da virus informatici, l'antivirus installato su ogni computer non deve mai essere disattivato o sostituito con altro antivirus. In caso di sospetta presenza di virus o di effettiva rilevazione, è necessario farne immediata segnalazione.

TRATTAMENTI SENZA L'AUSILIO DI STRUMENTI ELETTRONICI

I documenti cartacei, soprattutto se contenenti dati sensibili, devono essere custoditi in appositi armadi chiusi a chiave. Quando si ritiene che tali documenti debbano essere eliminati, procedere con la loro efficace distruzione attraverso l'uso, ad esempio, di dispositivi distruggi documenti.
Si raccomanda di custodire la documentazione cartacea in sicurezza al fine di evitare accessi impropri, perdita, divulgazione e distruzione dei dati e, nel caso di assenza anche momentanea dalla propria postazione di lavoro, chiudere le porte con le chiavi e custodire fascicoli, cartelle e documenti cartacei contenenti dati personali degli interessati negli appositi armadi anch'essi chiusi a chiave; di custodire gli atti e i documenti affidati per lo svolgimento dei propri compiti provvedendo alla tempestiva restituzione al termine delle attività; in caso di movimentazione, soprattutto di documentazione sanitaria, avere cura che essa avvenga previa verifica dell'effettiva correlazione della documentazione con l'interessato, utilizzando idonee cautele quali buste o pacchi chiusi o contenitori non trasparenti comunque privi di espliciti riferimenti a persone e prestazioni sanitarie erogate, riportando possibilmente la dicitura "RISERVATO"; evitare di riutilizzare, per ragioni di risparmio e di sensibilità ambientale, fogli non più utilizzati contenenti dati personali per i quali non sia più necessaria la conservazione; nel caso, non utilizzarli come carta per prendere appunti e, prima di essere conferiti nella raccolta differenziata, rendere non intelligibili i dati contenuti anche attraverso l'ausilio di dispositivi distruggi documenti.
Evitare il deposito di documenti di qualsiasi genere negli ambienti di transito o comunque accessibili a terzi (corridoi, sale d'attesa, luoghi di passaggio, ecc.). La documentazione contenente dati personali di uso quotidiano, che per ragioni di praticità operativa viene lasciata sulla scrivania, deve essere rimossa al termine della giornata lavorativa e conservata in armadi o cassetti chiusi a chiave.
Prestare particolare attenzione alla documentazione stampata a mezzo di stampanti condivise, avendo cura di recuperarla nell'immediatezza dell'operazione di stampa. Il numero di copie di documenti contenenti dati personali deve essere strettamente funzionale alle esigenze di lavoro.
Si raccomanda, in caso di allontanamento dal proprio ufficio o dalla propria postazione di lavoro, di adottare tutte le accortezze e precauzioni al fine di impedire l'accesso fisico a chi non sia legittimato, soprattutto se esterno all'organizzazione aziendale.
Al termine della giornata lavorativa, ove il contesto, la dinamica delle attività ed il numero di occupanti lo consentano, è necessario chiudere sempre a chiave gli uffici nei quali vengono svolti trattamenti di dati personali.