REGIONE DEL VENETO
ULSS2 MARCA TREVIGIANA

ISTRUZIONI OPERATIVE
PER GLI INCARICATI DEL TRATTAMENTO DEI DATI PERSONALI

In ottemperanza alle disposizioni del Regolamento UE 2016/679 per la protezione dei dati personali (GDPR 2016/679) e al Decreto Legislativo 196/2003, come modificato dal Decreto Legislativo 101/2018, si comunica che:

- l'Azienda ULSS 2 Marca Trevigiana, in qualità di **TITOLARE del trattamento di dati personali** *(di seguito "**Titolare**")*, ossia quale soggetto che determina le finalità e i mezzi dei trattamenti di dati personali effettuati nel proprio ambito, è tenuta a delineare al proprio interno un'adeguata ed efficace articolazione dei presidi e responsabilità a livello organizzativo, tenuto conto delle dimensioni e della complessità dell'Azienda stessa, al fine di assicurare il rispetto delle disposizioni del GDPR ed il monitoraggio delle operazioni di trattamento e delle attività di adempimento dei correlati obblighi normativi svolte dalle proprie strutture e dal personale;
- con deliberazione n. 1820 del 25.10.2018 l'Azienda ULSS n. 2 ha approvato il "Regolamento concernente la protezione dei dati personali", pubblicato nel sito istituzionale – sezione privacy (https://www.aulss2.veneto.it/privacy) e nel sito istituzionale – Amministrazione Trasparente (https://www.aulss2.veneto.it/amministrazione-trasparente/disposizioni-generali/atti-generali/regolamenti), e individuato ai sensi dell'art. 18 del citato Regolamento aziendale – in base all'organizzazione stabilita dal vigente Atto Aziendale – quale Incaricato del trattamento dei dati, in relazione alle funzioni di specifica competenza derivanti dal rapporto giuridico esistente con la stessa Azienda , tutto il personale dipendente, convenzionato o comunque che svolge operazioni di trattamento su dati di cui l'Azienda ha la titolarità.

Per quanto sopra riportato la S.V. in qualità di Incaricato del trattamento dei dati è tenuta ad osservare le presenti Istruzioni Operative.

TRATTAMENTO DI DATI PERSONALI

L'Art. 4 del GDPR 2016/679 definisce il trattamento di dati personali come "*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.*"

A tal fine i dati personali devono essere trattati:

a) secondo modalità tali da garantire la riservatezza;
b) in modo lecito, corretto e trasparente nei confronti dell'interessato, raccogliendo i dati per finalità determinate, esplicite e legittime;
c) limitatamente a quanto necessario rispetto alle finalità per le quali sono stati raccolti;
d) in modo da garantire un'adeguata sicurezza, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentale;
e) per un periodo di tempo non superiore a quello necessario agli scopi per i quali sono stati raccolti o successivamente trattati.

OBBLIGHI FORMALI

Ogni soggetto autorizzato al trattamento dei dati è tenuto a:

- attuare le misure necessarie per un corretto, lecito, sicuro trattamento, attenendosi alle istruzioni operative ed alle prescrizioni definite nella regolamentazione aziendale;
- tenere aggiornato l'elenco dei trattamenti a Lei affidati con le indicazioni relative alla tipologia dei dati trattati, alle banche dati, agli strumenti elettronici, all'ubicazione di detti strumenti e degli archivi informatici e cartacei;
- utilizzare le banche dati informatiche esclusivamente attraverso le proprie credenziali di autenticazione da tenere riservate, richiedere l'autorizzazione al proprio Delegato per le modifiche e/o integrazioni del profilo autorizzativo che si rendessero necessarie;
- disporre quanto necessario a garantire la sicurezza dei locali di trattamento ed archiviazione dei dati, adottando idonee misure contro accessi non autorizzati;
- ottemperare agli obblighi di informazione e acquisizione del consenso, quando non altrimenti eseguito dalla struttura nei confronti degli interessati;
- controllare e custodire, durante il compimento dell'intero trattamento e fino alla consegna, gli atti e i documenti contenenti dati, personali sensibili o giudiziari, in modo da impedirne l'accesso a persone non autorizzate;
- informare il proprio Delegato in merito alle eventuali richieste dell'interessato di esercitare i diritti previsti dagli artt. 12, 13 e 14 del GDRP 2016/679.

Per quanto non specificato si rinvia espressamente al "Regolamento concernente la protezione dei dati personali".

ACCESSO BANCHE DATI E DIVIETO DI DUPLICAZIONE BANCHE DATI

L'accesso alle banche dati è limitato agli utilizzi previsti dalle competenze attribuite al soggetto autorizzato. Non sono ammesse duplicazioni di data base contenenti dati personali, se non previa autorizzazione del Titolare o del Delegato.

UTILIZZO E TRASMISSIONE DEI DATI

I dati oggetto di trattamento non devono essere condivisi, comunicati o inviati a persone che non ne necessitano per lo svolgimento delle proprie attività lavorative. Nessun dato personale può essere utilizzato o trasmesso all'esterno senza previa autorizzazione del Titolare o del Delegato.

STRUMENTI INFORMATICI

Al fine di garantire un corretto trattamento dei dati nel rispetto delle misure di sicurezza che l'Azienda ha ritenuto idoneo adottare, è opportuno impiegare gli strumenti elettronici ed informatici con diligenza ed attenzione, attenendosi alle disposizioni contenute nel "Regolamento concernente l'utilizzo dei sistemi informatici aziendali", reso disponibile all'atto dell'assunzione e consultabile nel sito dell'Azienda ULSS n. 2 Marca trevigiana all'indirizzo: https://www.aulss2.veneto.it/atti-amministrativi-generali.

A compendio di quanto indicato nel suddetto regolamento, sono comunque impartite queste direttive:

- il trattamento di dati personali con strumenti elettronici è consentito alle figure dotati di credenziali di autenticazione (password riservata) che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti;
- i criteri di impostazione delle credenziali di autenticazione, così come la tempistica di cambiamento delle stesse, vengono comunicate dal Titolare del trattamento e/o di un suo delegato in relazione alla natura dei dati trattati e ai rischi sottesi a tali trattamenti;
- non è consentito comunicare a nessuno le proprie password e soprattutto le stesse non vanno scritte su supporti facilmente rintracciabili e soprattutto in prossimità della postazione di lavoro utilizzata;
- non è consentito lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento;
- non è consentito installare sulla propria postazione di lavoro programmi non attinenti alle normali attività d'ufficio né nuovi programmi necessari senza la preventiva autorizzazione del Titolare del trattamento e/o del suo delegato;
- non è consentito modificare le configurazioni hardware e software senza autorizzazione del Titolare del trattamento o del suo Delegato;
- se si rileva un problema nell'ambito dell'utilizzo del sistema informatico relativo al trattamento di dati in corso, che possa compromettere la sicurezza dei dati, si deve darne immediata comunicazione al Responsabile del sistema informativo;
- accertarsi che sul proprio computer sia sempre operativo un programma antivirus, aggiornato e con la funzione di monitoraggio attiva;
- sottoporre a controllo con il programma antivirus installato sul proprio PC, tutti i supporti di provenienza esterna prima di eseguire files in essi contenuti;
- accertarsi sempre della provenienza dei messaggi di posta elettronica contenenti allegati; nel caso che il mittente dia origine a dubbi, cancellare direttamente il messaggio senza aprire gli allegati;
- non è consentito scaricare da Internet programmi o file non inerenti l'attività lavorativa o comunque sospetti;
- utilizzare la connessione ad Internet esclusivamente per lo svolgimento dei propri compiti istituzionali;
- segnalare qualsiasi anomalia o stranezza di comportamento Titolare del trattamento e/o ad un suo delegato.

CREDENZIALI

Per il trattamento dei dati con gli strumenti elettronici in dotazione alla struttura il soggetto autorizzato viene dotato di credenziali di accesso (*username* e *password*).
Tali credenziali sono strettamente personali ed identificano l'operatore nella rete informatica.
Le caratteristiche e le norme da applicarsi a tutte le credenziali in uso al soggetto autorizzato, sono definite nel "Regolamento concernente l'utilizzo dei sistemi informatici aziendali", reso disponibile all'atto dell'assunzione e consultabile nel sito dell'Azienda ULSS n. 2 Marca trevigiana all'indirizzo: https://www.aulss2.veneto.it/atti-amministrativi-generali.

DOCUMENTI CARTACEI

I dati presenti su documenti cartacei devono essere tutelati mediante conservazione e gestione degli stessi in modo da evitarne la visibilità, la sottrazione, la riproduzione, l'alterazione o distruzione abusiva. Devono essere osservate le seguenti norme:

- i documenti contenenti dati personali, devono essere custoditi in modo da non essere accessibili a persone non incaricate del trattamento (*es. armadi o cassetti chiusi a chiave, uffici chiusi a chiave*);
- il documenti contenenti dati personali che vengono prelevati dagli archivi per l'attività quotidiana devono esservi riposti a fine giornata;
- i documenti contenenti dati personali non devono rimanere incustoditi su scrivanie stampanti, fotocopiatrici, fax o tavoli di lavoro;
- i documenti contenenti dati personali non devono essere condivisi, comunicati o inviati a persone che non ne necessitano per lo svolgimento delle proprie competenze lavorative (*anche se queste persone sono a loro volta soggetti autorizzati del trattamento*);
- qualora sia necessario distruggere i documenti contenti dati personali, questi devono essere distrutti utilizzando gli appositi apparecchi "distruggi documenti" o, in assenza, devono essere sminuzzati in modo da non essere più ricomponibili;
- i documenti che contengono dati sensibili e/o giudiziari devono essere controllati e custoditi dagli incaricati, i quali devono impedire l'accesso a persone prive di autorizzazione;
- l'archiviazione dei documenti cartacei contenenti dati sensibili e/o giudiziari deve avvenire in locali ad accesso controllato, utilizzando armadi o cassetti chiusi a chiave.