REGIONE DEL VENETO
ULSS2 MARCA TREVIGIANA

Treviso - data contratto / regolamento	Protocollo n. ///	Allegati n.

OGGETTO: Soggetto autorizzato privacy (artt. 17 e 19 del regolamento aziendale).
Atto di nomina – istruzioni operative e compiti.

VISTO il regolamento aziendale concernente la protezione dei dati personali, approvato con deliberazione n. 203 del 3.2.2023;

CONSIDERATO che il Regolamento Europeo (UE) 2016/679 dispone che il trattamento dei dati possa essere effettuato esclusivamente da parte di soggetti autorizzati;

RITENUTO che per l'ambito di attribuzioni, funzioni e competenze conferite, la S.V. abbia i requisiti di esperienza, capacità ed affidabilità idonei a garantire il pieno rispetto delle vigenti disposizioni in materia di trattamento dei dati ivi compreso il profilo relativo alla sicurezza;

IL DIRETTORE GENERALE
IL COORDINATORE PRIVACY
IL REFERENTE PRIVACY
IL DELEGATO PRIVACY

secondo l'ambito di afferenza con il presente atto

NOMINA LA S.V.

SOGGETTO AUTORIZZATO PRIVACY ai sensi degli artt. 17 e 19 del citato regolamento aziendale in materia, approvato con deliberazione n. 203 del 3.2.2023 e pubblicato nel sito istituzionale:

- sezione privacy – https://www.aulss2.veneto.it/privacy
- Amministrazione Trasparente – https://www.aulss2.veneto.it/amministrazione-trasparente/disposizioni-generali/atti-generali/regolamenti

per accedere ai dati personali necessari per lo svolgimento degli incarichi affidati nell'ambito dell'area / servizio / ufficio di assegnazione e a svolgere le operazioni di trattamento su tali dati nei limiti di quanto necessario ai fini dello svolgimento dei suddetti incarichi.

Nella sezione privacy – https://www.aulss2.veneto.it/privacy sono altresì reperibili tutte le informazioni, dati e documenti in materia di privacy.

La S.V., nella qualità sopra indicata, ha il compito e la responsabilità di adempiere a tutto quanto necessario per il rispetto delle disposizioni vigenti in materia e di osservare scrupolosamente quanto in essa previsto, nonché le allegate istruzioni operative e compiti.

Per tutto quanto non espressamente previsto nel presente atto, si rinvia alle disposizioni generali vigenti in materia di protezione dei dati personali.

SOGGETTO AUTORIZZATO PRIVACY
istruzioni operative e compiti relativi alla gestione delle attività di trattamento dei dati personali ai sensi dell'art. 29, Reg. (UE) 2016/679 (c.d. GDPR) e dell'art. 2-*quaterdecies*, D.Lgs. n. 196/2003 (c.d. Codice in materia di protezione dei dati personali).

INFORMAZIONI GENERALI

L'Azienda ULSS n. 2 Marca trevigiana, (di seguito "ULSS 2") è tenuta a mettere in atto misure tecniche e organizzative adeguate a garantire, ed essere in grado di dimostrare, che il trattamento è effettuato in conformità alla disciplina in materia di protezione dei dati personali.

Sotto il profilo organizzativo, ULSS 2 ritiene di dover individuare ciascuno dei collaboratori che, a vario titolo, è autorizzato a svolgere operazioni di trattamento sotto la propria autorità.

Oltre a ciò, ULSS 2 è tenuta a delineare al proprio interno un'adeguata ed efficace articolazione dei presidi e responsabilità a livello organizzativo, al fine di assicurare il rispetto della disciplina in materia di protezione dei dati personali ed il monitoraggio delle operazioni di trattamento e delle attività di adempimento dei correlati obblighi normativi svolte dai propri autorizzati.

In tale prospettiva, ULSS 2 si è dotata di un modello organizzativo e ha definito un organigramma in materia di protezione dei dati personali (di seguito "Modello Organizzativo Privacy"), disponibile per la presa visione nel sito istituzionale:

- sezione privacy – https://www.aulss2.veneto.it/privacy
- Amministrazione Trasparente – https://www.aulss2.veneto.it/amministrazione-trasparente/disposizioni-generali/atti-generali/regolamenti.

AUTORIZZAZIONE AL TRATTAMENTO DEI DATI PERSONALI SOTTO L'AUTORITÀ DEL TITOLARE[1]

ULSS 2, per il tramite del Direttore Generale / Coordinatore privacy / Referente privacy / Delegato privacy di riferimento, affida alla S.V. il ruolo di **SOGGETTO AUTORIZZATO PRIVACY** assegnando le attività di seguito precisate, oltre che nel Modello Organizzativo Privacy.

Fermo quanto sopra, nell'effettuare operazioni di trattamento dei dati dovrà conformarsi ai seguenti principi generali:

- il trattamento di dati personali può essere svolto soltanto per le finalità e con le modalità strettamente correlate allo svolgimento delle attività affidate nell'ambito dell'area / servizio / ufficio di assegnazione / riferimento e secondo le prassi seguite da ULSS 2;
- è consentito l'accesso ai soli dati personali strettamente necessari all'esecuzione delle predette attività;
- è necessario verificare che i dati trattati siano esatti e completi e procedere, se necessario, alla loro correzione o al loro aggiornamento, controllando altresì che siano pertinenti e non eccedenti rispetto alle attività svolte ed ai compiti assegnati;
- è necessario osservare gli adempimenti previsti dalla vigente normativa in materia di protezione dei dati personali, per quanto di propria competenza, applicando le istruzioni impartite da ULSS 2 e la modulistica eventualmente messa a disposizione;
- è necessario mantenere e garantire la riservatezza sui dati personali trattati e, in generale, sulle informazioni comunque apprese nello svolgimento delle proprie attività, astenendosi dal comunicarli a terzi se non nei casi previsti dalle prassi da ULSS 2;
- in caso di cessazione dell'attività lavorativa, è necessario astenersi dall'effettuare operazioni di trattamento dei dati personali conosciuti durante lo svolgimento dell'incarico e, in particolare, dal conservarli, duplicarli, comunicarli, o cederli a terzi;

[1] Salvo diversa indicazione, il presente documento si intende applicabile anche nei casi in cui l'Azienda ULSS n. 2 operasse quale responsabile o contitolare del trattamento, con esclusione delle parti non compatibili con tale ruolo.

- è doveroso informare prontamente la Figura Privacy di riferimento (es. Delegato Privacy) circa ogni questione rilevante in relazione al trattamento di dati personali effettuato o eventuali richieste ricevute dalle persone a cui si riferiscono i dati (gli Interessati);
- è necessario attenersi alle istruzioni e misure di sicurezza presenti in regolamenti / linee guida predisposti in ambito aziendale, in modo da evitare i rischi di perdita o distruzione (anche accidentale) dei dati, di trattamento non consentito o non conforme alla finalità per cui i dati sono raccolti, anche nel rispetto degli standard di sicurezza seguiti da ULSS 2.

Si rammenta che la violazione delle disposizioni in materia di protezione dei dati personali può esporre ULSS2, quale titolare del trattamento, a responsabilità civile, penale e amministrativa.

ISTRUZIONI OPERATIVE E COMPITI

Al fine di evitare rischi di accesso non autorizzato o non consentito, perdita, distruzione o danneggiamento dei dati (anche accidentali), le persone autorizzate al trattamento dei dati personali devono attenersi a tutte le prescrizioni e misure di sicurezza che vengono qui di seguito riportate:

1) Controllare e custodire gli strumenti elettronici utilizzati per il trattamento dei dati e i documenti contenenti dati personali, di cui si è a conoscenza o in possesso per lo svolgimento delle attività e dei compiti assegnati, in modo tale da impedire l'accesso a persone non autorizzate o trattamenti non consentiti.
2) Curare la gestione delle credenziali d'autenticazione secondo le specifiche procedure ed istruzioni operative previste dai manuali e documenti aziendali, attenendosi inoltre alle seguenti disposizioni:
   a) utilizzare il codice identificativo (user-id) e la password riservata assegnati per l'accesso ai dati trattati mediante strumenti elettronici e custodirli diligentemente garantendone la segretezza;
   b) la password deve esser composta da una sequenza di almeno otto caratteri (normali e speciali) sia numerici che alfabetici (o, se il programma in uso non lo permetta, dal numero massimo di caratteri consentito);
   c) nella generazione della password, si deve prestare la massima attenzione a non utilizzare elementi o notizie facilmente riconducibili all'utilizzatore; devono quindi, ad esempio, esser evitati riferimenti a: nome e cognome, data di nascita, numero di matricola, nome di familiari, numero di telefono di casa o dell'ufficio, soprannomi noti, nonché nomi di personaggi famosi, ecc.;
   d) la password deve essere modificata al primo utilizzo ed ogni volta che viene richiesto dal sistema (al massimo: 6 mesi per i dati personali e 3 mesi per quelli particolari[2]), ovvero ogniqualvolta vi sia il dubbio che ne sia stata violata la segretezza. Nella generazione della nuova password, non devono essere utilizzate sequenze di caratteri già usate in precedenza;
   e) la password deve rimanere assolutamente riservata. A tale fine, deve essere evitata la digitazione in presenza di terzi ed è necessaria la conservazione in luogo non accessibile ad altri (va dunque assolutamente evitata l'apposizione sul video-terminale di biglietti o adesivi contenti riferimenti alla password). Va altresì evitato l'uso di sistemi automatici di inserimento di password (es. macro o predisposizione tasti funzione);
   f) la password non può essere comunicata, per nessun motivo, ai colleghi del proprio o di altri uffici.
3) In tutti i casi di allontanamento, anche temporaneo, dalla postazione di lavoro (es: pausa pranzo), è necessario bloccare la propria sessione di lavoro. Tale accorgimento deve essere adottato soprattutto in caso di utilizzazione, da parte di più soggetti autorizzati, della medesima postazione di lavoro.
4) Tutte le persone autorizzate al trattamento dei dati devono partecipare attivamente agli eventuali interventi formativi in materia di privacy organizzati da ULSS 2 e devono riferire alla Figura Privacy di riferimento (es. Delegato Privacy) ogni e qualsiasi anomalia riscontrata nell'esercizio della propria attività.
5) I trattamenti di dati contenuti in atti e documenti cartacei devono essere svolti garantendo sempre la corretta custodia degli stessi. I documenti non possono, pertanto, esser lasciati incustoditi sulla propria scrivania e/o in luoghi aperti al pubblico in assenza di altri soggetti autorizzati addetti al medesimo trattamento; non devono essere consultati da altri soggetti autorizzati non abilitati al trattamento; non possono essere riprodotti o fotocopiati se non per esigenze connesse alla finalità del trattamento; non possono essere portati al di fuori dei locali individuati per la loro conservazione se non in casi del tutto

[2] Si tratta delle seguenti categorie di dati: dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona (art. 9 GDPR).

eccezionali e, qualora si procedesse in tal senso, l'asportazione dovrà essere ridotta al tempo minimo necessario per effettuare le operazioni di trattamento. Al termine dell'orario di lavoro, la persona autorizzata al trattamento deve, inoltre, riportare tutti i documenti cartacei contenenti dati personali nei locali individuati per la loro conservazione.

6) Qualora sia necessario distruggere i documenti cartacei 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.
7) È proibito comunicare dati personali per telefono, se non si è certi che il destinatario sia una persona autorizzata al trattamento dei dati personali in questione.
8) In tutte le ipotesi in cui venga utilizzata una stampante condivisa da vari utenti situata al di fuori dei locali ove è posta la singola stazione di lavoro, alle operazioni di stampa sarà possibile procedere soltanto previa verifica della assenza, nei locali ove è sita la stampante, di soggetti non autorizzati al trattamento. Le stampe devono essere raccolte immediatamente e custodite con le modalità descritte nei punti precedenti.
9) È fatto assoluto divieto di entrare in locali ad accesso limitato, se non previa espressa autorizzazione del relativo responsabile.
10) Qualora sia effettuato un trattamento di eventuali categorie particolari di dati personali e/o di dati personali relativi a condanne penali e reati, ogni persona autorizzata al trattamento è, inoltre, tenuta a:
    a) custodire tutti i supporti rimovibili su cui sono memorizzati eventuali categorie particolari di dati personali e dati personali relativi a condanne penali e reati (usb pen drive, dvd rom, cd rom, ecc.) in modo da evitare accessi e trattamenti non autorizzati;
    b) distruggere i suddetti supporti rimovibili al termine del loro utilizzo, ovvero cancellare definitivamente le informazioni in essi registrate prima di un loro riutilizzo;
    c) custodire i documenti contenenti particolari di dati personali e dati personali relativi a condanne penali e reati in archivi chiusi a chiave e limitandone l'accesso alle sole persone preventivamente autorizzate;
    d) restituire i documenti contenenti tali dati al termine delle operazioni di trattamento ai soggetti incaricati della relativa archiviazione.

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".