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

FRONTESPIZIO DELIBERAZIONE

AOO: AS_BO66

REGISTRO: Deliberazione

NUMERO: 0000275

DATA: 21/12/2018 18:07

OGGETTO: REGOLAMENTO (UE) 2016/679. DEFINIZIONE DELL'ORGANIGRAMMA AZIENDALE: REFERENTI PRIVACY (E RELATIVE FUNZIONI), SOGGETTI AUTORIZZATI AL TRATTAMENTO DEI DATI PERSONALI e GRUPPO AZIENDALE PRIVACY. APPROVAZIONE ISTRUZIONI OPERATIVE GENERALI.

SOTTOSCRITTO DIGITALMENTE DA:

Il presente atto è stato firmato digitalmente da Rossi Andrea in qualità di Direttore Generale
Con il parere favorevole di Dall'Olmi Emanuela - Direttore Sanitario
Con il parere favorevole di Donattini Maria Teresa - Direttore Amministrativo

CLASSIFICAZIONI:

- [07-05]

DESTINATARI:

- Collegio sindacale
- DIREZIONE MEDICA DI PRESIDIO
- FORMAZIONE
- SERVIZIO UNICO METROPOLITANO AMMINISTRAZIONE DEL PERSONALE
- UO SEGRETERIA GENERALE E AFFARI LEGALI
- UO TECNOLOGIE INFORMATICHE E DI RETE
- DIPARTIMENTO CURE PRIMARIE

DOCUMENTI:

File	Firmato digitalmente da	Hash
DELI0000275_2018_delibera_firmata.pdf	Dall'Olmi Emanuela; Donattini Maria Teresa; Rossi Andrea	629AB8772EEBB97B94B1821800C946B6F2611A6D8000C8BF919E9F2C4D66A8F4
DELI0000275_2018_Allegato1.docx:		6D713C4E1F853D8D2D196B3D1C5129124DF1BB90B7B9D726A09A0DFF29DAA116
DELI0000275_2018_Allegato2.docx:		0BB6FF91916A0503BA3289F903D528A4803CBB0EA90487163425DBF39B53E6D5
DELI0000275_2018_Allegato3.docx:		B5A53E6256C74E408D3B5F9415BD1055A53337B2EFEAE24B2D257317C697C6FD

DELIBERAZIONE

OGGETTO: REGOLAMENTO (UE) 2016/679. DEFINIZIONE DELL'ORGANIGRAMMA AZIENDALE: REFERENTI PRIVACY (E RELATIVE FUNZIONI), SOGGETTI AUTORIZZATI AL TRATTAMENTO DEI DATI PERSONALI e GRUPPO AZIENDALE PRIVACY. APPROVAZIONE ISTRUZIONI OPERATIVE GENERALI.

IL DIRETTORE GENERALE

PREMESSO CHE:

- il Regolamento (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati (in seguito per brevità "GDPR"), applicabile in tutti gli Stati membri dell'Unione Europea a partire dal 25 maggio 2018, nell'affrontare il tema della tutela dei dati personali attraverso un approccio basato principalmente sulla valutazione dei rischi sui diritti e le libertà degli interessati, attribuisce ai Titolari del trattamento il compito di assicurare ed essere in grado di comprovare il rispetto dei principi applicabili al trattamento dei dati personali e di adottare le misure che ritiene a ciò più idonee ed opportune (c.d. principio di responsabilizzazione o accountability);
- il richiamato GDPR detta una complessa disciplina di carattere generale in materia di protezione dei dati personali, prevedendo molteplici obblighi ed adempimenti a carico dei soggetti che trattano dati personali, ivi comprese le Aziende Sanitarie;
- il "sistema privacy" delineato dal GDPR implica la necessità di infondere nell'organizzazione aziendale la piena consapevolezza dei rischi inerenti ai trattamenti, nonché l'affermazione di una cultura della protezione dei dati quale parte integrante dell'intero asset informativo di un'organizzazione, con particolare attenzione ai dati di salute (ivi compresi i dati biometrici e genetici);
- tale nuovo approccio deve coinvolgere tutti i soggetti chiamati a trattare i dati personali all'interno della organizzazione aziendale, con assunzione delle relative responsabilità;

- visto il decreto legislativo n.101 /2018 "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio Europeo;

- richiamata la DGR Regione Emilia Romagna n. 919 del 10/4/2018 "Linee di programmazione e di finanziamento delle Aziende e degli enti del Servizio Sanitario regionale per l'anno 2018" che prevede fra gli obiettivi indicati al punto 4.6 dell'allegato B, oltre la nomina del DPO e l'adozione del registro delle attività di trattamento, la ri-definizione e l'articolazione delle specifiche responsabilità privacy aziendali;

- Richiamate inoltre:
- la Delibera n. 142 del 29.6.2018 di nomina del Data Protection Officer (DPO);
- la deliberazione n. 265 del 21.12.2017 che istituisce l'Ufficio per la transizione al digitale nell'ambito dell'UO Tecnologie Informatiche e di rete, affidandone la responsabilità al relativo Direttore, con attribuzione dei compiti elencati alll'art. 17 del Codice dell'amministrazione digitale;
- la precedente deliberazione n. 98 del 4.7.2016 "D.Lgs. 196/2003. Documento per la sicurezza. Aggiornamento 2015-2016" e il successivo "Documento Misure minime di sicurezza ICT per le pubbliche amministrazioni – Circolare AGID 18 aprile 2017, n.2/2017" di cui al prot. 38935 del 22.12.2017;

- Considerato che oltre al DPO, il GDPR - con riferimento ai soggetti - disciplina espressamente le figure del " **titolare del trattamento**" e del " **responsabile del trattamento**", intendendosi con quest'ultima espressione i soggetti esterni alla organizzazione che trattano dati personali per conto del titolare del trattamento;

- Considerato altresì che

- il medesimo GDPR non prevede le figure del "responsabile [interno] del trattamento" e dell' "incaricato" del trattamento (come in precedenza individuati dagli artt. 29 e 30 del D. Lgs. 196/2003 - Codice Privacy), e introduce la categoria delle "persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare [...]" (art. 4, n. 10);
- a sua volta, l'Autorità Garante per la protezione dei dati personali "ritiene opportuno che titolari [.....] del trattamento mantengano in essere la struttura organizzativa e le modalità di designazione degli incaricati di trattamento così come delineatesi negli anni" (cfr. Guida all´applicazione del Regolamento europeo in materia di protezione dei dati personali);
- l'art. 2 quaterdecies del D. Lgs. 196/2003, introdotto dal D.lgs. n.101 del 10.8.2018, recita " Il titolare o il responsabile del trattamento possono prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità". I comma " Il Titolare o il responsabile del trattamento individuano le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta" II comma;

- Richiamato l'art. 4 del GDPR che definisce **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";

- Rilevato che il titolare del trattamento, ai sensi dell'art. 32 del GDPR, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, mette in atto misure tecniche ed organizzative adeguate per garantire un livello di sicurezza adeguato al rischio;

- Rilevato, inoltre, che gli artt. 29 e 32 del GDPR dispongono che chiunque agisca sotto l'autorità del titolare del trattamento e abbia accesso a dati personali possa trattare tali dati solo se adeguatamente istruito;

- Ritenuto pertanto, alla luce delle premesse, delle novità introdotte dal GDPR, dal D.Lgs. 101/2018 e delle raccomandazioni del Garante Privacy sopra richiamate, di dover garantire continuità rispetto alle scelte organizzative negli anni assunte dalla Azienda, aggiornando tuttavia e potenziando l'organigramma privacy aziendale, da ultimo definito con Delibera n.264 del 21/12/2017, in termini di attribuzioni di compiti e funzioni derivanti dal GDPR, e utilizzando altresì una terminologia in linea con il GDPR;

- Precisato, quanto all'assetto delle responsabilità, che:

- con deliberazione n. 108 del 21 settembre 2004 sono stati individuati i trattamenti di dati personali/sensibili/giudiziari di titolarità aziendale, riportati nel Documento Allegato 1 della citata deliberazione; sono stati nominati i Responsabili ex art. 29 del D.Lgs. 196/2003, coincidenti con i Direttori delle strutture (Unità Operative/Servizi/Articolazioni) alle quali fanno capo per competenza i singoli trattamenti, come individuate nel citato Documento Allegato 1; sono state approvate le istruzioni operative per i Responsabili dei trattamenti (Documento Allegato n.2 alla suddetta delibera), con definizione dei compiti assegnati in particolare sotto il profilo delle misure di sicurezza (minime ed idonee) per i trattamenti senza l'ausilio di strumenti elettronici (art.31 e 35 e Allegato B del D.Lgs.196) e sotto il profilo dell'individuazione e nomina degli incaricati, istruzioni poi aggiornate con la deliberazione n. 151 del 24.12.2008; i dipendenti sono stati incaricati ex art.30 D.Lgs. 196/2003 di tutti i trattamenti senza l'ausilio di strumenti elettronici facenti capo alla struttura (Unità Operativa/Servizio) alla quale i dipendenti medesimi sono formalmente assegnati (fatte salve le diverse determinazioni dei Responsabili di trattamento); è stato approvato il modello di istruzione operativa per gli incaricati (ex art.30 D.Lgs. 196), Allegato n.3 alla citata deliberazione, riportante il contenuto minimo dei compiti/obblighi applicabile alla generalità dei trattamenti a prescindere dal profilo di incarico, integrabile a cura dei Responsabili se necessario in relazione alle caratteristiche dei trattamenti e/o alle mansioni degli incaricati, istruzioni aggiornate con deliberazione n. 151 del 24.12.2008; - è stata confermata la nomina del Direttore dell'Unità Operativa Tecnologie Informatiche e di Rete quale Responsabile ex art.29 del D.Lgs. 196/2003 di tutti i trattamenti di dati con strumenti elettronici previsti nel citato Documento Allegati 1 alla deliberazione, in affiancamento agli ulteriori Responsabili nominati con il medesimo provvedimento; è stato incaricato il gruppo di lavoro aziendale di diffondere la deliberazione suddetta ed è stato dato mandato all'Unità Operativa Risorse Umane di formalizzare le nomine dei Responsabili di trattamento per il futuro, in caso di

variazioni soggettive nella titolarità delle strutture aziendali come individuate nel richiamato Documento Allegato 1;

- la deliberazione n. 104 è stata annualmente aggiornata quanto a ricognizione dei trattamenti, delle U.O. Responsabili e dei dirigenti responsabili di trattamento nonché degli incaricati, anche ai sensi e per gli effetti di cui all'art. 35, comma 1, lett. a) del D.Lgs. 196/2003, ai sensi del quale è misura minima di sicurezza l'"aggiornamento periodica dell'individuazione dell'ambito di trattamento consentito ai singoli incaricati o alle unità organizzative";
- da ultimo l'aggiornamento annuale è stato effettuato con la richiamata deliberazione n. 264 del 21.12.2017, che si conferma fino alla data di adozione della presente deliberazione nell'assetto organizzativo e funzionale ivi previsto;

- Ritenuto di confermare l'attribuzione di compiti e funzioni in materia di protezione dati (come più avanti precisate) alle figure apicali della Dirigenza (ex Responsabili interni), in linea con l'organizzazione aziendale sopra descritta risalente al 2004, sia pure estendendo (in un'ottica di maggiore garanzia del sistema) il ruolo di **Referente privacy** a tutto il personale con incarico di direzione di Unità operativa complessa, semplice dipartimentale e di programma gestionale, oltre che ai Responsabili delle Tecnostrutture in staff alla Direzione;

- dato atto che i compiti e le funzioni attribuiti ai referenti privacy sono elencati nel documento allegato 1 alla presente deliberazione "Compiti, funzioni e poteri dei referenti privacy";

- ritenuto di dare mandato al competente SUMAP, di trasmettere la presente deliberazione, a tutti i dirigenti attualmente titolari degli incarichi dirigenziali sopra descritti e per il futuro, a seguito di ogni conferimento/rinnovo o comunque di variazioni soggettive nella titolarità degli incarichi come sopra individuati;

- dato atto che ciascun direttore/responsabile assume il ruolo di Referente privacy per le attività di trattamento afferenti all'U.O diretta, come risultanti dal Registro dei trattamenti e dalle funzioni attribuite all'U.O. specificate nell'Atto aziendale di cui al D. Lgs. 502, nel Regolamento attuativo e nelle successive delibere di integrazione/modifica;

- ritenuto inoltre, con riferimento specifico alle previgenti figure degli incaricati del trattamento, di confermare l'assetto attuale e pertanto di autorizzare al trattamento dei dati personali tutti i soggetti che operano sotto la diretta autorità del Titolare del trattamento, e quindi tutti i dipendenti ed i titolari di rapporto di lavoro autonomo (se ed in quanto operanti stabilmente nell'ambito delle strutture aziendali), ivi compresi i borsisti, gli specialisti ambulatoriali e di continuità assistenziale, attribuendo loro la qualifica di "soggetti autorizzati al trattamento dei dati" (**Autorizzati**) con riferimento ai dati afferenti all'U.O. (complessa, o semplice dipartimentale, "Programma gestionale" o Tecnostruttura in staff alla Direzione) cui sono formalmente addetti, come risultanti dal Registro dei trattamenti e dalle funzioni attribuite all'U.O. di

appartenenza specificate nell'Atto aziendale di cui all'art. 3 D. Lgs.502, nel relativo Regolamento attuativo e nelle successive delibere di integrazione/modifica;

- dato atto che la comunicazione di tale autorizzazione al trattamento a tutti i dipendenti ed alle categorie di personale sopra elencate avverrà mediante messa a disposizione della presente deliberazione nel Profilo Personale del Portale del dipendente (GRU), oltre che tramite pubblicazione nell'intranet aziendale e nel sito internet sezione "privacy", dando mandato al SUMAP e al DCP, secondo le rispettive competenze, di procedere analogamente nei confronti del personale di nuova "assunzione" , integrando altresì i (futuri) contratti di lavoro con apposita clausola;

- precisato che per i trattamenti di dati con procedura informatizzata l'attivazione delle credenziali di autenticazione informatica per il personale autorizzato di cui sopra resta in capo al Referente privacy di afferenza che deve specificare a quali dati e tipi di operazioni ciascun autorizzato può accedere in relazione ai propri compiti e la conseguente disattivazione in caso di cessazione (se non automaticamente collegata al profilo);

- ritenuto inoltre di qualificare come "soggetti autorizzati al trattamento" anche gli specializzandi e gli studenti dei corsi di studio delle professioni sanitarie gestiti in convenzione con UNIBO, con riferimento alle attività di trattamento di dati afferenti all'U.O (complessa, o semplice dipartimentale, "Programma gestionale" o tecnostruttura in staff) cui sono addetti nell'ambito del percorso formativo, come risultanti dal Registro dei trattamenti e dalle funzioni attribuite all'U.O. di appartenenza specificate nell'Atto aziendale di cui all'art.3 D. Lgs.502, nel relativo Regolamento attuativo e nelle successive delibere di integrazione/modifica;

- dato atto che la comunicazione di tale autorizzazione al trattamento, compete al responsabile della Formazione per gli studenti e alla Direzione medica di presidio per gli specializzandi;

- precisato inoltre che l'autorizzazione al trattamento del personale non rientrante nelle categorie sopra citate, non stabilmente operante all'interno delle strutture aziendali, (a titolo esemplificativo: frequentatori volontari, volontari, lavoratori socialmente utili) sarà data di volta in volta, ad personam, a cura del Referente privacy/Direttore-Responsabile della struttura alla quale afferisce tale personale, che provvederà utilizzando la modulistica allegata (all. 3 "Atto di designazione del soggetto autorizzato al trattamento dei dati personali").

- considerato che tutti i soggetti autorizzati al trattamento dei dati operano sotto la diretta autorità del Titolare e sulla base di indicazioni ricevute anche dal rispettivo Referente privacy e che svolgono le operazioni di trattamento, secondo le istruzioni generali impartite dal Titolare, come riportate all'allegato 2 che riporta il contenuto minimo dei compiti-obblighi applicabile alla generalità dei trattamenti a prescindere dai profili dell'incarico, fermo restando che i referenti sono tenuti ad integrare e dettagliare tale schema se necessario in base alle caratteristiche specifiche dei singoli trattamenti o in base alle mansioni dei singoli operatori autorizzati"

- tenuto conto che i principi generali in tema di trattamento dei dati e le istruzioni richiamate, integrano le istruzioni/informazioni/indicazioni/direttive di carattere generale che il Titolare rende disponibili nella sezione della rete intranet aziendale dedicata Normative e Regolamenti - Privacy, e che, anche alla luce del quadro normativo in evoluzione, è fatto obbligo a ciascun soggetto autorizzato al trattamento di consultare gli aggiornamenti della documentazione aziendale in materia, sul sito intranet aziendale nella sezione sopra citata.

- precisato che, in applicazione del Codice di Comportamento di questa Azienda, approvato con Deliberazione n. 112 del 25 maggio 2018 nonché delle disposizioni dei vigenti CCNL della Dirigenza e del CCNL Comparto Sanità, la mancata osservanza da parte del personale autorizzato delle disposizioni poste dalla normativa in materia di trattamento dei dati personali costituisce condotta perseguibile da parte dell' Ufficio competente per i procedimenti disciplinari ai sensi dell'art.55 e ss del D. Lgs. 165/01.

- dato atto che il Titolare si avvale del DPO, nominato con la deliberazione citata, al quale sono attribuiti i seguenti compiti:

- informa e fornisce consulenza alle Aziende/Enti, in ordine agli obblighi derivanti dal Regolamento, nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati. Per il tramite dei referenti/responsabili privacy aziendali individuati dalle singole Aziende/Enti dovrà altresì assicurare attività di informazione/consulenza ai Responsabili del trattamento nonché ai dipendenti che, in qualità di autorizzati al trattamento, eseguono operazioni di trattamento dati;
- sorveglia l'osservanza della normativa in materia di protezione dei dati personali nonché delle policy aziendali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti, coordinando il gruppo dei referenti/responsabili privacy aziendali individuati dalle singole Aziende/Enti;
- fornisce, se richiesti, pareri anche scritti in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento;
- coopera con l'Autorità Garante per la protezione dei dati personali, fungendo da punto di contatto per la stessa per questioni connesse al trattamento (tra cui la consultazione preventiva) ed effettuare eventuali consultazioni e curarne in generale i rapporti;
- supporta le strutture aziendali deputate alla tenuta del Registro del trattamento delle singole Aziende/Enti al fine di uniformarne la predisposizione;
- garantisce il corretto livello di interlocuzione con gli altri DPO delle Aziende sanitarie regionali e/o con il DPO della Regione Emilia-Romagna in relazione a progetti ed iniziative di valenza regionale/metropolitana (ad es. FSE, ARA, GRU, GAAC);
- promuove iniziative congiunte tra le Aziende/Enti affinchè l'applicazione della normativa in materia di protezione dei dati personali nonché delle policy aziendali sia sviluppata secondo linee applicative omogenee e coerenti nelle singole Aziende/Enti;

- favorisce il coordinamento dei DPO delle altre aziende sanitarie regionali relativamente alle tematiche precedentemente presidiate dal Tavolo Privacy Regionale, come da richiesta della Regione Emilia-Romagna, nota PG/2018/0482475 del 5 luglio 2018.

- dato atto inoltre che nell'organizzazione aziendale è da tempo istituito il Gruppo aziendale privacy (GAP), coordinato dal Direttore dell'UOSGAL e dal Direttore dell'UOTIR e costituito da componenti in rappresentanza delle macro aree aziendali, amministrativa, ospedaliera, territoriale, infermieristica;

- ritenuto che la combinazione delle conoscenze giuridiche, informatiche, organizzative e specialistiche di ciascuna area, rappresenti il giusto approccio multidisciplinare e che sia pertanto da confermare il ruolo del gruppo aziendale privacy, che si rinnova nella seguente composizione:

Coordinamento in capo al Direttore dell'UOSGAL e a un dirigente dell'UOTIR designato dal Direttore dell'U.O.
Componenti:
- un dirigente/funzionario designato dal Direttore amministrativo, per l'area amministrativa (Dipartimento amministrativo e uffici staff Direzione: Informazione e Comunicazione, Formazione, Programmazione e Controllo direzionali, Ricerca e Innovazione, Governo clinico, Medicina legale);
- un dirigente medico di organizzazione designato dal Direttore della Direzione medica di Presidio, per l'area ospedaliera
- un rappresentante designato dal Direttore del DIT, per l'area infermieristica
- due dirigenti/funzionari designati dal Direttore sanitario per Distretto, DCP, DSM e DSP;

- preso atto della non sussistenza di oneri conseguenti al presente provvedimento a carico del redigendo bilancio economico preventivo dell'anno in corso;

- acquisito il parere favorevole della Dott.ssa Federica Banorri in qualità di DPO, in atti al prot. n. 39482/2018;

Delibera

per le motivazioni esposte in premessa e che si intendono qui integralmente riportate:

1. di designare Referenti privacy i Direttori delle U.O. Complesse e delle U.O.S. dipartimentali, nonché i Responsabili dei programmi gestionali e delle Tecnostrutture in staff alla Direzione aziendale, ciascuno per le attività di trattamento afferenti all'UO/struttura diretta, come derivanti dal Registro dei trattamenti di cui all'art. 30 GDPR e dalle funzioni proprie di ogni U.O/struttura descritte nell'Atto aziendale di cui al D.Lgs. 502, nel Regolamento attuativo (deliberazione n. 4 del 14.1.2009) e nelle successive delibere di integrazione/modifica;

2. di attribuire ai Referenti privacy le funzioni dettagliate nel documento allegato 1 alla presente deliberazione “Compiti, funzioni e poteri dei referenti privacy”;

3. di dare mandato al SUMAP di trasmettere la presente deliberazione ai Dirigenti attualmente titolari degli incarichi dirigenziali di cui al punto 1 e di procedere analogamente per il futuro, a seguito di ogni conferimento/rinnovo o comunque di variazioni soggettive nella titolarità degli incarichi come sopra individuati, integrando altresì il contratto individuale con apposita clausola;

4. di autorizzare al trattamento dei dati personali tutti i soggetti che operano sotto la diretta autorità del Titolare del trattamento, e quindi tutti i dipendenti ed i titolari di rapporto di lavoro autonomo (se ed in quanto operanti stabilmente nell’ambito delle strutture aziendali), ivi compresi i borsisti ,gli specialisti ambulatoriali e di continuità assistenziale, attribuendo loro la qualifica di “soggetti autorizzati al trattamento dei dati” con riferimento ai trattamenti afferenti all’U.O. (complessa, o semplice dipartimentale, Programma gestionale o tecnostruttura in staff) cui sono formalmente addetti, come risultanti dal Registro dei trattamenti aziendale e dalle funzioni attribuite all’U.O. di afferenza, specificate nell’Atto aziendale di cui al D. Lgs.502, nel relativo Regolamento attuativo e nelle successive delibere di integrazione/modifica (fatta salva la facoltà del Referente privacy di circoscrivere l’autorizzazione generale se in relazione alla natura dei dati ed al rapporto di strumentalità tra dati/finalità e mansioni del singolo lavoratore detta autorizzazione generale risulti eccedente);

5. di comunicare l’autorizzazione al trattamento a tutti i dipendenti ed alle categorie di personale elencate al precedente punto 4 mediante messa a disposizione della presente deliberazione nel Profilo Personale del Portale del dipendente (GRU), oltre che tramite pubblicazione nell’intranet aziendale e nel sito internet sezione “privacy”; dando mandato al SUMAP e al DCP, secondo le rispettive competenze, di procedere analogamente nei confronti del personale di nuova “assunzione” integrando altresì i (futuri) contratti di lavoro con apposita clausola;

6. di autorizzare inoltre al trattamento dei dati personali gli studenti dei corsi di studio delle professioni sanitarie gestiti in convenzione con UNIBO e gli specializzandi attribuendo loro la qualifica di “soggetti autorizzati al trattamento dei dati” con riferimento ai trattamenti afferenti all’U.O. (complessa, o semplice dipartimentale, programma gestionale o tecnostruttura in staff) in cui sono inseriti nel corso del programma formativo, come risultanti dal Registro dei trattamenti aziendale e dalle funzioni attribuite all’U.O. di afferenza specificate nell’Atto aziendale di cui al D. Lgs.502, nel relativo Regolamento attuativo e nelle successive delibere di integrazione/modifica (fatta salva la facoltà del Referente privacy di circoscrivere l’autorizzazione generale se in relazione alla natura dei dati ed al rapporto di strumentalità tra dati/finalità e percorso formativo detta autorizzazione generale risulti eccedente);;

7. di dare mandato di comunicare l’autorizzazione al trattamento alle categorie di cui al punto 6, alla Tecnostruttura Formazione per gli studenti e alla Direzione medica di Presidio per gli specializzandi;

8. di dare atto che l'autorizzazione al trattamento per il personale non rientrante nelle categorie di cui al punto 4 e al punto 6 (a titolo esemplificativo: tirocinanti, frequentatori volontari), non operante stabilmente nelle strutture aziendali, è ad personam e che deve provvedere il referente privacy/Direttore (o Responsabile) dell'Unità Operativa cui afferisce tale personale con utilizzo della modulistica allegata alla presente deliberazione (allegato 3 "Atto di designazione del soggetto autorizzato al trattamento dei dati personali");

9. di approvare le istruzioni operative generali per tutti i soggetti autorizzati al trattamento dei dati, nel testo allegato n. 2 alla presente deliberazione, quale contenuto minimo di compiti, modelli comportamentali, obblighi applicabili alla generalità dei trattamenti ed a prescindere dai profili di abilitazione, fermo restando che i referenti privacy sono tenuti a integrare e dettagliare tale schema se necessario in base alle caratteristiche specifiche dei singoli trattamenti o in base alle specifiche mansioni dei soggetti autorizzati;

10. di confermare il gruppo aziendale privacy (GAP) , nella seguente composizione:

- coordinatori: Direttore dell'UOSGAL e un dirigente dell'UOTIR (designato dal Direttore);
- area ospedaliera: un dirigente medico di organizzazione designato dal Direttore del Presidio ospedaliero;
- area amministrativa (UU.OO. del Dipartimento amministrativo e tec. e uffici in staff alla direzione): 1-2 dirigenti o funzionari designati dal Direttore amministrativo;
- area territoriale: n. 2 dirigenti o funzionari designati dal Direttore Sanitario per Distretto, Dipartimento Cure Primarie, Dipartimento salute mentale, Dipartimento sanità Pubblica;
- area infermieristica: un rappresentante designato dal Direttore DIT;

11. di dare atto che, ferma la composizione di cui sopra, il gruppo è così costituito (eventuali variazioni soggettive saranno disposte con le modalità sopra indicate):

- coordinatori: Sabrina Fiorentini (direttore SGAL) e Monica Nanni (dirigente presso TIR)
- area amministrativa: Piani Morena (Direzione) e Alba Fontana (DAT)
- area ospedaliera: Zarabini Lucia
- area territoriale: Gasparetto Stefania e Michela Cavallo
- area infermieristica: Ivana Nanni

12. di attribuire al gruppo aziendale privacy (GAP) il compito di assicurare un presidio aziendale per gli adempimenti organizzativi e procedurali derivanti dalle nuove disposizioni normative in materia di protezione dei dati personali. Il GAP ha i seguenti compiti:

- supportare i Referenti aziendali privacy nell'adozione delle misure adeguate ed efficaci per la tutela della riservatezza, integrità e disponibilità del patrimonio informativo come individuate dall'azienda, a

seguito degli approfondimenti e delle analisi effettuate dai coordinatori del GAP con il DPO nel Tavolo di area metropolitana e unitamente al Responsabile della transizione digitale/Direttore UOTIR;

- supportare i Referenti aziendali privacy, nell'aggiornamento del Registro dei trattamenti di dati personali effettuati dalle strutture di appartenenza e nella eventuale valutazione di impatto;
- fornire supporto alle verifiche di sicurezza svolte dall'UOTIR e/o dal DPO;
- coordinare le richieste di parere al DPO da parte dei singoli Referenti Aziendali Privacy;

13. di confermare i compiti attribuiti al Responsabile per la transizione digitale con la deliberazione n. 265 del 21.12.2017;

14. di confermare i compiti attribuiti al DPO di seguito elencati:

- informa e fornisce consulenza alle Aziende/Enti, in ordine agli obblighi derivanti dal Regolamento, nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati. Per il tramite dei referenti/responsabili privacy aziendali individuati dalle singole Aziende/Enti dovrà altresì assicurare attività di informazione/consulenza ai Responsabili del trattamento nonché ai dipendenti che, in qualità di autorizzati al trattamento, eseguono operazioni di trattamento dati;
- sorveglia l'osservanza della normativa in materia di protezione dei dati personali nonché delle policy aziendali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti, coordinando il gruppo dei referenti/responsabili privacy aziendali individuati dalle singole Aziende/Enti;
- fornisce, se richiesti, pareri anche scritti in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento;
- coopera con l'Autorità Garante per la protezione dei dati personali, fungendo da punto di contatto per la stessa per questioni connesse al trattamento (tra cui la consultazione preventiva) ed effettuare eventuali consultazioni e curarne in generale i rapporti;
- supporta le strutture aziendali deputate alla tenuta del Registro del trattamento delle singole Aziende/Enti al fine di uniformarne la predisposizione;
- garantisce il corretto livello di interlocuzione con gli altri DPO delle Aziende sanitarie regionali e/o con il DPO della Regione Emilia-Romagna in relazione a progetti ed iniziative di valenza regionale/metropolitana (ad es. FSE, ARA, GRU, GAAC);
- promuove iniziative congiunte tra le Aziende/Enti affinchè l'applicazione della normativa in materia di protezione dei dati personali nonché delle policy aziendali sia sviluppata secondo linee applicative omogenee e coerenti nelle singole Aziende/Enti;
- favorisce il coordinamento dei DPO delle altre aziende sanitarie regionali relativamente alle tematiche precedentemente presidiate dal Tavolo Privacy Regionale, come da richiesta della Regione Emilia-Romagna, nota PG/2018/0482475 del 5 luglio 2018.

15. di trasmettere copia della presente deliberazione al Collegio Sindacale ai sensi dell’art. 18, comma 4 della L.R. 16.7.2018 n. 9;

COMPITI FUNZIONI E POTERI DEI REFERENTI PRIVACY

- Trattare i dati personali solo su istruzione del Titolare del trattamento e garantire la corretta applicazione del Regolamento generale per la protezione dei dati (GDPR) e del D.Lgs. 196/2003, come modificato dal D.Lgs.101/2018, nonché la conformità alle indicazioni dell'Autorità Garante per la protezione dei dati personali;
- Osservare e fare osservare:
    a) le direttive aziendali in materia di protezione, di finalità, di modalità di trattamento dei dati, fornite dal Titolare del trattamento, anche per il tramite del Gruppo Aziendale Privacy e dell'U.O. Tecnologie Informatiche e di Rete (UO TIR);
    b) le istruzioni di carattere generale impartire dal Titolare a tutti i soggetti autorizzati al trattamento (di cui all'**allegato 2**);
    c) eventuali ulteriori specifiche istruzioni predisposte dallo stesso in relazione agli specifici ambiti di competenza, anche per gruppi omogenei di funzioni.

- Porre in atto all'interno della propria struttura organizzativa le procedure e le linee guida aziendali per la corretta gestione dei dati, assicurando che i soggetti interessati (es. pazienti, dipendenti, fornitori…..) ricevano le informazioni relative al trattamento dei dati personali di cui agli artt.13 e 14 del GDPR;
- Provvedere alla designazione dei soggetti autorizzati al trattamento dei dati personali per i singoli operatori per i quali tale autorizzazione non può essere rilasciata contestualmente alla sottoscrizione di un contratto di lavoro/incarico (a titolo non esaustivo: frequentatori volontari, lavoratori socialmente utili,……..), attraverso la predisposizione dell'apposito modello di cui l'**allegato 3**;
- Vigilare sulla conformità dell'operato dei soggetti autorizzati ad essi afferenti alle istruzioni e alle direttive di cui sopra, verificando periodicamente lo stato di adeguamento alla normativa in oggetto;
- Verificare che i dati oggetto di trattamento siano esatti, aggiornati, indispensabili, pertinenti e non eccedenti rispetto alle finalità per cui vengono trattati;
- Attenersi alle indicazioni di sicurezza dettate dal Titolare del trattamento e compatibilmente con l'ambito di attività, adottare le misure di sicurezza tecniche e soprattutto organizzative adeguate, al fine di proteggere i dati da trattamenti non autorizzati o illeciti, dal rischio di perdita, di distruzione o di danno accidentale;
- Partecipare ai momenti formativi organizzati dall' Azienda ed assicurare la partecipazione dei propri autorizzati;
- Fornire le informazioni richieste dal Gruppo Aziendale Privacy, e segnalare al medesimo ogni questione rilevante in materia e trasmettere tempestivamente istanze e reclami degli interessati, da far pervenire al DPO;
- Comunicare al Gruppo Aziendale Privacy, i trattamenti in essere all'interno del proprio settore di competenza, l'inizio di ogni nuovo trattamento e la cessazione o modifica di quelli esistenti, ai fini della compilazione e del continuo aggiornamento del Registro dei trattamenti aziendale;
- Collaborare con l'U.O. TIR per la predisposizione del documento della valutazione di impatto sulla protezione dei dati qualora ne ricorrano i presupposti in base all'art. 35 del GDPR;
- Non porre in essere trattamenti di dati diversi e ulteriori senza la preventiva autorizzazione del Titolare del trattamento;
- Provvedere, qualora tra le attività istituzionali della Struttura vi sia la stipula di contratti/convenzioni con soggetti esterni alla organizzazione che comportino il trattamento di dati personali per conto del Titolare del trattamento, alla contestuale stipula o predisposizione del relativo atto di designazione di tali soggetti esterni quali "responsabili del trattamento" a norma dell'art. 28 del GDPR e delle condizioni ivi indicate e trasmettere copia dell'atto di designazione e dell'accettazione della nomina al Gruppo Aziendale

Privacy, anche ai fini dell’aggiornamento del registro aziendale delle attività di trattamento dei dati;

- Comunicare tempestivamente al Gruppo Aziendale Privacy i potenziali casi di data breach all'interno della propria struttura e collaborare alla istruttoria del caso al fine di sottoporre al DPO ogni utile e opportuna determinazione in merito;

Allegato 2

ISTRUZIONI di CARATTERE GENERALE impartire dal Titolare a tutti i SOGGETTI AUTORIZZATI AL TRATTAMENTO DEI DATI PERSONALI

Principi Generali

1. Trattare i dati di propria competenza nel rispetto dei principi di liceità, correttezza e trasparenza.
2. In attuazione del:
    a. principio di minimizzazione dei dati: trattare i soli ed esclusivi dati personali che si rilevino necessari rispetto alle finalità per le quali sono trattati nell'attività a cui ciascun autorizzato è preposto;
    b. principio di limitazione delle finalità: trattare i dati conformemente alle finalità istituzionali del Titolare, limitando il trattamento esclusivamente a dette finalità;
    c. principio di esattezza: garantire l'esattezza, la disponibilità, l'integrità nonché il tempestivo aggiornamento dei dati personali oggetto di trattamento e verificare la pertinenza, completezza e non eccedenza rispetto alle finalità per le quali sono stati raccolti, e successivamente trattati.
3. Utilizzare le informazioni e i dati personali, in particolare i dati c.d. particolari con la massima riservatezza sia nei confronti dell'esterno che del personale interno, per tutta la durata dell'incarico ed anche successivamente al termine di esso.
4. Conservare i dati rispettando le misure di sicurezza, predisposte dal Titolare e/o dal Referente privacy di afferenza garantendone la massima protezione in ogni attività di trattamento.
5. Segnalare al Referente privacy di afferenza eventuali circostanze che rendano necessario od opportuno l'aggiornamento delle predette misure di sicurezza al fine di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.
6. Astenersi dal comunicare a terzi e/o a diffondere dati ed informazioni appresi in occasione dell'espletamento della propria attività.
7. Partecipare ai corsi formativi in materia di protezione dei dati personali e di sicurezza informatica con le modalità che verranno indicate dal Titolare del trattamento o suo delegato.

Istruzioni operative

ISTRUZIONI PER LO SVOLGIMENTO DELLE OPERAZIONI CARATTERIZZANTI IL PROCESSO DI TRATTAMENTO

- identificazione degli interessati: nell'ambito dell'accesso alle prestazioni, l'autorizzato al trattamento può avere necessità di dover identificare il richiedente un servizio o il soggetto che deve presentare una istanza o una dichiarazione. Si deve procedere a tale verifica con rispetto della volontà dell'interessato, che deve essere invitato con cortesia ad esibire un

proprio documento di identità, secondo quanto previsto dall'art.45 del DPR 445/2000 e nel rispetto di eventuali indicazioni operative aziendali;

- raccolta dei dati: prima di procedere all'acquisizione dei dati personali deve essere fornita l'informativa all'interessato o alla persona presso cui si raccolgono i dati, secondo quanto stabilito dagli artt.13 e 14 del Regolamento (UE) 2016/679. Occorre procedere alla raccolta dei dati con la massima cura, verificando l'esattezza dei dati stessi;
- registrazione dei dati: non lasciare a disposizione di estranei supporti, fogli, cartelle e quant'altro;
- al momento della consegna di copie dei documenti ai destinatari è necessario adottare tutte le garanzie di sicurezza, quali l'utilizzo di buste sigillate e l'eventuale acquisizione della delega se presente. L'invio di comunicazioni o di documentazione sanitaria al domicilio del paziente deve essere sempre preceduto dall'autorizzazione di questi ed essere sempre contenuto in busta sigillata, evitando di riportare sulla busta esterna riferimenti a servizi/strutture specifici dell'Azienda che possano in qualche modo essere idonee a rivelare lo stato di salute dell'interessato o a creare una forma di associazione con una qualsivoglia patologia.

ISTRUZIONI PER IL CORRETTO UTILIZZO DEGLI STRUMENTI AZIENDALI PER IL TRATTAMENTO DEI DATI PERSONALI

- Per le banche dati informatiche, utilizzare sempre il proprio codice di accesso personale, evitando di operare su terminali a disposizione altrui e/o di lasciare avviato, in caso di allontanamento anche temporaneo dalla postazione di lavoro, il sistema operativo con inserita la propria password, al fine di evitare trattamenti non autorizzati e di consentire sempre l'individuazione dell'autore del trattamento;
- email e uso della internet: la posta elettronica può essere utilizzata per scopi di ufficio. Occorre prestare particolare attenzione alla spedizione, a mezzo di posta elettronica, di files o di messaggi contenti dati riferiti alla salute. A tal specifico fine si rinvia alle disposizioni aziendali.
- uso di software: è vietato installare e usare qualunque software senza la previa autorizzazione del Titolare e/o Suo delegato. Si ricorda che l'uso di software contraffatto, ovvero senza licenza d'uso, costituisce un illecito di natura sia penale sia civile, secondo quanto previsto dalla legge sul diritto d'autore (legge 633/1941), così come integrata dal d.lgs.518/1992 e ss.mm. ed ii..
- protezione degli strumenti di lavoro: in caso di assenza, anche momentanea, dalla propria postazione di lavoro, devono essere adottate misure idonee ad escludere che soggetti non autorizzati possano acquisire la conoscenza di informazioni o accedere alle banche dati. A tal proposito, a titolo meramente esemplificativo, si consiglia di adottare un sistema di oscuramento (c.d. screensaver) dotato di password, ovvero di uscire dal programma che si sta utilizzando o, in alternativa, occorrerò porre lo strumento elettronico in dotazione in posizione di stand-by o spegnere l'elaboratore che si sta utilizzando. In caso di abbandono, anche temporaneo, dell'ufficio, l'autorizzato deve porre la massima attenzione a non lasciare incustoditi i documenti cartacei contenenti dati riferiti alla salute e altri tipologie di dati c.d "particolari" (es. adesione ad un sindacato) sulla scrivania o su tavolini di reparto: è infatti necessario identificare un luogo sicuro di custodia che dia adeguate garanzie di protezione da accessi non autorizzati (un armadio o un cassetto chiusi a chiave, una cassaforte, ecc.);

ISTRUZIONI RIGUARDANTI RAPPORTI DI FRONT OFFICE

- Rispetto della distanza di sicurezza: per quanto riguarda gli operatori di sportello deve essere prestata attenzione al rispetto dello spazio di cortesia e se del caso devono essere invitati gli utenti a sostare dietro la linea tracciata sul pavimento ovvero dietro le barriere delimitanti lo spazio di riservatezza;
- obbligo di riservatezza e segretezza: mantenere l'assoluta segretezza sulle informazioni di cui venga a conoscenza nel corso delle operazioni di trattamento. La diffusione di dati idonei a rivelare lo stato di salute è tassativamente vietata;
- controllo dell'identità del richiedente nel caso di richieste di comunicazioni di dati (presentate per telefono): occorre verificare l'identità del soggetto richiedente, ad esempio formulando una serie di quesiti (accertamento sommario).

Gli obblighi sopra descritti fanno parte integrante della prestazione lavorativa e pertanto per il personale dipendente o assimilato sono dovuti in base al contratto di lavoro sottoscritto con l'Azienda/Istituto.

Le suddette istruzioni sono integrabili dai singoli Referenti Privacy di afferenza attraverso ulteriori istruzioni di carattere specifico, anche per gruppi omogenei di funzioni.

Le istruzioni di cui sopra sono altresì integrate dalle puntuali disposizioni aziendali in materia di protezione dei dati personali (quali il Regolamento per il corretto utilizzo dei sistemi informatici aziendali e la procedura Dossier Sanitario elettronico) a cui si rinvia, reperibili sempre alla pagina intranet dedicata.

ATTO DI DESIGNAZIONE
DEL SOGGETTO AUTORIZZATO AL TRATTAMENTO DEI DATI PERSONALI

Ai sensi dell'art. 2-quaterdecies del D.Lgs. n. 196/2003, così come modificato dal D.Lgs. n. 101/2018

Il sottoscritto_____

(indicare il nome del Referente Privacy di afferenza)

in qualità di Referente Privacy dell' UO/UOC/……_____

DESIGNA

(indicare NOME e COGNOME)

in qualità di ……

(indicare funzione, ruolo,…)

SOGGETTO AUTORIZZATO AL TRATTAMENTO DEI DATI relativi

AMBITO DEL TRATTAMENTO (sede/i di assegnazione) DESCRIZIONE DEL TRATTAMENTO ARCHIVI BANCHE DATI

A seguito della suddetta designazione Lei è autorizzato a svolgere operazioni di trattamento, per il proprio ambito di competenza, secondo i principi generali di trattamento, le prescrizioni, le istruzioni operative generali impartite dal Titolare e le ulteriori eventuali istruzioni specifiche dal sottoscritto impartite.

Principi di carattere generale:

- ✓ trattare i dati di propria pertinenza in modo lecito, secondo correttezza e trasparenza;
- ✓ trattare i soli dati necessari allo svolgimento delle operazioni da effettuare;
- ✓ verificare che i dati personali siano pertinenti, completi e non eccedenti le finalità per le quali sono stati raccolti e successivamente trattati;
- ✓ conservarli nel rispetto delle misure di sicurezza previste dal Regolamento (UE) n. 2016/679, dalle istruzioni di carattere generale impartite dal Titolare (**allegate alla presente**) e sempre consultabili nella sezione Privacy della rete intranet aziendale, dalle prescrizioni e dalle ulteriori eventuali misure di sicurezza impartite dal sottoscritto in qualità di Referente Privacy di Sua afferenza.

Prescrizioni:

a. Rispettare l'obbligo di riservatezza e segretezza, mantenendo la segretezza delle informazioni di cui venga a conoscenza mediante accesso ai sistemi informativi aziendali, secondo il profilo di autorizzazione assegnato alle proprie credenziali di autenticazione (user e password), corrispondente alla classe di autorizzato di appartenenza;
b. trattare i dati di propria pertinenza in modo lecito, secondo correttezza e trasparenza;
c. trattare i soli dati necessari allo svolgimento delle operazioni da effettuare;
d. verificare che i dati personali siano pertinenti, completi e non eccedenti le finalità per le quali sono stati raccolti e successivamente trattati;
e. conservare i dati nel rispetto delle misure di sicurezza previste dal Regolamento (UE) n. 2016/679, dalle istruzioni di carattere generale impartite dal Titolare, consultabili nella

sezione Privacy della rete intranet aziendale, e dalle ulteriori eventuali misure di sicurezza impartite dal sottoscritto;

f. utilizzare le informazioni e i dati, con cui si entra in contatto per ragioni di lavoro, esclusivamente per lo svolgimento delle attività istituzionali, con la massima riservatezza, secondo quanto definito dalle regole aziendali, per tutta la durata dell'incarico ed anche successivamente al termine di esso, astenendosi dal comunicare a terzi dati e informazioni (salvo i casi previsti dalla legge);
g. per le banche dati informatiche, utilizzare sempre il proprio codice di accesso personale, evitando di operare su tutti dispositivi in dotazione ad altri operatori e/o di lasciare, in caso di allontanamento anche temporaneo dalla postazione di lavoro il sistema operativo avviato con inserita la propria password, al fine di evitare trattamenti non autorizzati e di consentire sempre l'individuazione dell'autore del trattamento;
h. conservare correttamente i supporti informatici e/o cartacei contenenti i dati personali in modo da evitare che gli stessi siano accessibili a persone non autorizzate mettendo in atto tutte le misure di sicurezza previste dal Regolamento Europeo in materia di protezione dei dati n. 2016/679, dalla normativa nazionale, dalle istruzioni di carattere generale impartite dal Titolare, consultabili nella sezione sopra indicata, e dalle ulteriori eventuali misure di sicurezza impartite dal sottoscritto;
i. astenersi dal comunicare a terzi dati e informazioni (salvo i casi previsti dalla legge);
j. segnalare al sottoscritto eventuali circostanze che rendano necessario od opportuno l'aggiornamento delle predette misure di sicurezza, al fine di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;
k. informare senza ingiustificato ritardo il soggetto delegato al trattamento di qualunque fatto o circostanza, anche accidentale, che abbia causato perdita, distruzione dei dati, accesso non consentito o comunque non conforme ai principi sopradetti.

La S.V. prende atto di quanto previsto nella presente designazione ed assume la qualifica di soggetto autorizzato al trattamento dei dati personali impegnandosi a:

- ✓ rispettare i principi e le prescrizioni sopraripportate, le istruzioni di carattere generale impartite dal Titolare, allegate al presente atto di designazione e disponibili nella sezione Privacy della rete intranet aziendale, e le eventuali istruzioni che Le verranno eventualmente impartite per l'ambito di competenza e del profilo professionale di appartenenza.

E' fatto obbligo a ciascun professionista autorizzato al trattamento consultare gli aggiornamenti della documentazione aziendale in materia sul sito intranet aziendale nella sezione sopra citata.

Ciò premesso, il presente atto costituisce pertanto conferimento formale dell'autorizzazione al trattamento dei dati connessi allo svolgimento dell'attività lavorativa connessa all'ambito del trattamento sopra individuato, secondo le istruzioni allegate e secondo le prescrizioni sopra riportate. Tale DESIGNAZIONE:

- ha validità per l'intera durata del rapporto con l'Azienda;
- viene a cessare al modificarsi del rapporto o con esplicita revoca dello stesso.

DICHIARAZIONE DI RICEVIMENTO DELL'ATTO DI DESIGNAZIONE E DI IMPEGNO ALL'OSSERVANZA DELLE ISTRUZIONI ALLEGATE

Il sottoscritto _____

(indicare NOME e COGNOME)

DICHIARA

1. di aver ricevuto la designazione a autorizzato al trattamento;
2. di aver attentamente letto e compreso il contenuto del presente atto e del suo allegato, e di impegnarsi ad osservare tutte e specifiche istruzioni impartite;
3. di obbligarsi ad osservare le ulteriori direttive/regolamentazioni aziendali reperibili alla sezione intranet dedicata;
4. di assicurare che l'obbligo di riservatezza correlato all'incarico sarà osservato anche successivamente alla conclusione dello stesso

Data_____

Firma_____

Allegato

ISTRUZIONI di CARATTERE GENERALE impartire dal Titolare a tutti i SOGGETTI AUTORIZZATI AL TRATTAMENTO DEI DATI PERSONALI

Principi Generali

1. Trattare i dati di propria competenza nel rispetto dei principi di liceità, correttezza e trasparenza.
2. In attuazione del:
    a. principio di minimizzazione dei dati: trattare i soli ed esclusivi dati personali che si rilevino necessari rispetto alle finalità per le quali sono trattati nell'attività a cui ciascun autorizzato è preposto;
    b. principio di limitazione delle finalità: trattare i dati conformemente alle finalità istituzionali del Titolare, limitando il trattamento esclusivamente a dette finalità;
    c. principio di esattezza: garantire l'esattezza, la disponibilità, l'integrità nonché il tempestivo aggiornamento dei dati personali oggetto di trattamento e verificare la pertinenza, completezza e non eccedenza rispetto alle finalità per le quali sono stati raccolti, e successivamente trattati.
3. Utilizzare le informazioni e i dati personali, in particolare i dati c.d. particolari con la massima riservatezza sia nei confronti dell'esterno che del personale interno, per tutta la durata dell'incarico ed anche successivamente al termine di esso.
4. Conservare i dati rispettando le misure di sicurezza, predisposte dal Titolare e/o dal Referente privacy di afferenza garantendone la massima protezione in ogni attività di trattamento.
5. Segnalare al Referente privacy di afferenza eventuali circostanze che rendano necessario od opportuno l'aggiornamento delle predette misure di sicurezza al fine di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

6. Astenersi dal comunicare a terzi e/o a diffondere dati ed informazioni appresi in occasione dell'espletamento della propria attività.
7. Partecipare ai corsi formativi in materia di protezione dei dati personali e di sicurezza informatica con le modalità che verranno indicate dal Titolare del trattamento o suo delegato.

Istruzioni operative

ISTRUZIONI PER LO SVOLGIMENTO DELLE OPERAZIONI CARATTERIZZANTI IL PROCESSO DI TRATTAMENTO

- identificazione degli interessati: nell'ambito dell'accesso alle prestazioni, l'autorizzato al trattamento può avere necessità di dover identificare il richiedente un servizio o il soggetto che deve presentare una istanza o una dichiarazione. Si deve procedere a tale verifica con rispetto della volontà dell'interessato, che deve essere invitato con cortesia ad esibire un proprio documento di identità, secondo quanto previsto dall'art.45 del DPR 445/2000 e nel rispetto di eventuali indicazioni operative aziendali;
- raccolta dei dati: prima di procedere all'acquisizione dei dati personali deve essere fornita l'informativa all'interessato o alla persona presso cui si raccolgono i dati, secondo quanto stabilito dagli artt.13 e 14 del Regolamento (UE) 2016/679. Occorre procedere alla raccolta dei dati con la massima cura, verificando l'esattezza dei dati stessi;
- registrazione dei dati: non lasciare a disposizione di estranei supporti, fogli, cartelle e quant'altro;
- al momento della consegna di copie dei documenti ai destinatari è necessario adottare tutte le garanzie di sicurezza, quali l'utilizzo di buste sigillate e l'eventuale acquisizione della delega se presente. L'invio di comunicazioni o di documentazione sanitaria al domicilio del paziente deve essere sempre preceduto dall'autorizzazione di questi ed essere sempre contenuto in busta sigillata, evitando di riportare sulla busta esterna riferimenti a servizi/strutture specifici dell'Azienda che possano in qualche modo essere idonee a rivelare lo stato di salute dell'interessato o a creare una forma di associazione con una qualsivoglia patologia.

ISTRUZIONI PER IL CORRETTO UTILIZZO DEGLI STRUMENTI AZIENDALI PER IL TRATTAMENTO DEI DATI PERSONALI

- Per le banche dati informatiche, utilizzare sempre il proprio codice di accesso personale, evitando di operare su terminali a disposizione altrui e/o di lasciare avviato, in caso di allontanamento anche temporaneo dalla postazione di lavoro, il sistema operativo con inserita la propria password, al fine di evitare trattamenti non autorizzati e di consentire sempre l'individuazione dell'autore del trattamento;
- email e uso della internet: la posta elettronica può essere utilizzata per scopi di ufficio. Occorre prestare particolare attenzione alla spedizione, a mezzo di posta elettronica, di files o di messaggi contenti dati riferiti alla salute. A tal specifico fine si rinvia alle disposizioni aziendali.
- uso di software: è vietato installare e usare qualunque software senza la previa autorizzazione del Titolare e/o Suo delegato. Si ricorda che l'uso di software contraffatto, ovvero senza licenza d'uso, costituisce un illecito di natura sia penale sia civile, secondo quanto previsto dalla legge sul diritto d'autore (legge 633/1941), così come integrata dal d.lgs.518/1992 e ss.mm. ed ii..

- protezione degli strumenti di lavoro: in caso di assenza, anche momentanea, dalla propria postazione di lavoro, devono essere adottate misure idonee ad escludere che soggetti non autorizzati possano acquisire la conoscenza di informazioni o accedere alle banche dati. A tal proposito, a titolo meramente esemplificativo, si consiglia di adottare un sistema di oscuramento (c.d. screensaver) dotato di password, ovvero di uscire dal programma che si sta utilizzando o, in alternativa, occorrerò porre lo strumento elettronico in dotazione in posizione di stand-by o spegnere l'elaboratore che si sta utilizzando. In caso di abbandono, anche temporaneo, dell'ufficio, l'autorizzato deve porre la massima attenzione a non lasciare incustoditi i documenti cartacei contenenti dati riferiti alla salute e altri tipologie di dati c.d "particolari" (es. adesione ad un sindacato) sulla scrivania o su tavolini di reparto: è infatti necessario identificare un luogo sicuro di custodia che dia adeguate garanzie di protezione da accessi non autorizzati (un armadio o un cassetto chiusi a chiave, una cassaforte, ecc.);

ISTRUZIONI RIGUARDANTI RAPPORTI DI FRONT OFFICE

- Rispetto della distanza di sicurezza: per quanto riguarda gli operatori di sportello deve essere prestata attenzione al rispetto dello spazio di cortesia e se del caso devono essere invitati gli utenti a sostare dietro la linea tracciata sul pavimento ovvero dietro le barriere delimitanti lo spazio di riservatezza;
- obbligo di riservatezza e segretezza: mantenere l'assoluta segretezza sulle informazioni di cui venga a conoscenza nel corso delle operazioni di trattamento. La diffusione di dati idonei a rivelare lo stato di salute è tassativamente vietata;
- controllo dell'identità del richiedente nel caso di richieste di comunicazioni di dati (presentate per telefono): occorre verificare l'identità del soggetto richiedente, ad esempio formulando una serie di quesiti (accertamento sommario).

Gli obblighi sopra descritti fanno parte integrante della prestazione lavorativa e pertanto per il personale dipendente o assimilato sono dovuti in base al contratto di lavoro sottoscritto con l'Azienda/Istituto.

Le suddette istruzioni sono integrabili dai singoli Referenti Privacy di afferenza attraverso ulteriori istruzioni di carattere specifico, anche per gruppi omogenei di funzioni.

Le istruzioni di cui sopra sono altresì integrate dalle puntuali disposizioni aziendali in materia di protezione dei dati personali (quali il Regolamento per il corretto utilizzo dei sistemi informatici aziendali e la procedura Dossier Sanitario elettronico) a cui si rinvia, reperibili sempre alla pagina intranet dedicata.