FRONTESPIZIO DELIBERAZIONE

AOO: ASL_BO

REGISTRO: Deliberazione

NUMERO: 0000011

DATA: 14/01/2019 14:24

OGGETTO: ADEGUAMENTI AL REGOLAMENTO (UE) 2016/679. DEFINIZIONE DELL'ORGANIGRAMMA DELLE RESPONSABILITÁ PRIVACY AZIENDALI E MODALITÁ DI INDIVIDUAZIONE DEI REFERENTI PRIVACY AZIENDALI E DEI SOGGETTI AUTORIZZATI AL TRATTAMENTO DEI DATI PERSONALI.

SOTTOSCRITTO DIGITALMENTE DA:

Il presente atto è stato firmato digitalmente da Gibertoni Chiara in qualità di Direttore Generale
Con il parere favorevole di Novaco Francesca Caterina - Direttore Sanitario
Con il parere favorevole di Petrini Anna Maria - Direttore Amministrativo

Su proposta di Grazia Matarante - UO Anticorruzione, Trasparenza e Privacy (SC) che esprime parere favorevole in ordine ai contenuti sostanziali, formali e di legittimità del presente atto

CLASSIFICAZIONI:

- [01-01-02]

DESTINATARI:

- Collegio sindacale
- Direzione Generale
- Dipartimento Chirurgico
- Dipartimento Materno Infantile
- Dipartimento Oncologico
- DAAT - Dipartimento Attivita' Amministrative Territoriali
- Servizio Unico Metropolitano Amministrazione del Personale (SUMAP)
- UO Affari Generali e Legali (SC)
- UO Servizio Prevenzione e Protezione (SC)
- UO Igiene (SC)
- Direzione Attivita' Socio-Sanitarie - DASS (SC)
- Dipartimento Cure Primarie
- Dipartimento Salute Mentale - Dipendenze Patologiche
- Dipartimento Sanita' Pubblica
- Dipartimento Emergenza
- Dipartimento Medico

- Dipartimento Servizi
- IRCCS Istituto delle Scienze Neurologiche - Direzione Scientifica
- IRCCS Istituto delle Scienze Neurologiche - Direzione Operativa
- UOC Direzione Amministrativa IRCCS
- Dipartimento Amministrativo
- Dipartimento Tecnico-Patrimoniale
- Dipartimento Farmaceutico
- Servizio Unico Metropolitano Contabilita' e Finanza (SUMCF)
- Servizio Unico Metropolitano Economato (SUME)
- UO Libera Professione (SC)
- UO Anticorruzione, Trasparenza e Privacy (SC)
- UO Servizi Amministrativi Ospedalieri (SC)
- UO Funzioni HUB (SC)
- UO Presidio Ospedaliero Unico Aziendale (SC)
- UO Governo Clinico e Sistema Qualita' (SC)
- UO Controllo di Gestione e Flussi Informativi (SC)
- UO Sviluppo Organizzativo, Professionale e Formazione (SC)
- UO Medicina Legale e Risk Management (SC)
- UO Committenza e Specialistica Ambulatoriale (SC)
- UO Ingegneria Clinica (SC)
- Distretto di Committenza e Garanzia dell'Appennino Bolognese
- Distretto di Committenza e Garanzia della Citta' di Bologna
- UO Amministrativa DSM - DP (SC)
- Distretto di Committenza e Garanzia di San Lazzaro di Savena
- Distretto di Committenza e Garanzia Pianura Ovest
- Distretto di Committenza e Garanzia Reno, Lavino e Samoggia
- Distretto di Committenza e Garanzia Pianura EST
- DATeR - Direzione Assistenziale Tecnica e Riabilitativa
- UO Amministrativa e Segreteria DATeR (SSD)
- UO Amministrativa DSP (SC)
- UO Amministrativa DCP (SC)

DOCUMENTI:

File	Firmato digitalmente da	Hash
DELI0000011_2019_delibera_firmata.pdf	Gibertoni Chiara; Matarante Grazia; Novaco Francesca Caterina; Petrini Anna Maria	33ADD1E7F6F5600C81DBECA30FD74361 8E71F98503852E59C2AC1D352E5A9A0E
DELI0000011_2019_Allegato1.pdf:		9E979F511E505504AB8CC9FBD3B81578 BA532BA4DEBE4AA53F04C9197F74569F
DELI0000011_2019_Allegato2.pdf:		B8BB253C21ED3225D4119468F20375D96 FF338F80C1C494CAB06574456B8B018
DELI0000011_2019_Allegato3.pdf:		6C064700E06BCDF7EC3599DAB67D46AF 029DB7632BD831C37EC5D5D4528BFFD7

DELIBERAZIONE

OGGETTO: ADEGUAMENTI AL REGOLAMENTO (UE) 2016/679. DEFINIZIONE DELL'ORGANIGRAMMA DELLE RESPONSABILITÁ PRIVACY AZIENDALI E MODALITÁ DI INDIVIDUAZIONE DEI REFERENTI PRIVACY AZIENDALI E DEI SOGGETTI AUTORIZZATI AL TRATTAMENTO DEI DATI PERSONALI.

IL DIRETTORE GENERALE

Su proposta della Dr.ssa Grazia Matarante, Dirigente Amministrativo a tempo indeterminato, Direttore UO Anticorruzione, Trasparenza e Privacy (SC), la quale esprime contestuale parere favorevole in ordine ai contenuti sostanziali, formali e di legittimità del presente provvedimento;

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", General Data Protection Regulation), 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 e 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*);
- che 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, attribuendo al titolare il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati;
- che il Decreto Legislativo n.101 del 10 agosto 2018 recante disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio Europeo, in attuazione dell'art.13 della legge di delegazione europea 2016-2017 (legge 25 ottobre 2017, n.163) ha introdotto disposizioni per l'adeguamento della normativa nazionale alle disposizioni del GDPR, novellando il codice della privacy di cui al D.Lgs. n.196/2003;
- che il " *sistema privacy*" delineato dal GDPR e confermato a livello nazionale dal D.Lgs. n.101/2018 di modifica ed integrazione del D.Lgs. n.196/2003, 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* informa tivo di un'organizzazione, con particolare attenzione ai dati di salute (ivi compresi i dati biometrici e genetici);
- che il nuovo approccio comporta il coinvolgimento di tutti i soggetti chiamati a trattare i dati personali all'interno della organizzazione aziendale, con assunzione delle relative responsabilità;

- che la Regione Emilia-Romagna con DGR n.919 del 10/4/2018, avente ad oggetto “Linee di programmazione e di finanziamento delle Aziende e degli enti del Servizio Sanitario regionale per l’anno 2018” ha previsto, fra gli obiettivi indicati al punto 4.6 dell’allegato B, oltre alla nomina del Responsabile della Protezione dei Dati (RPD) - Data Protection Officer (DPO) e all’adozione del Registro delle attività di trattamento, la ridefinizione e l’articolazione delle specifiche responsabilità privacy aziendali;

Richiamate le deliberazioni dell’Azienda USL di Bologna:

- n.267 del 22 novembre 2005, recante “Determinazioni in merito agli adempimenti di cui al d.lgs. n.196/2003 Codice in materia di protezione dei dati personali”, di approvazione delle apposite linee di indirizzo e di programmazione aziendali;
- n.182 del 24/07/2013 avente ad oggetto: “Ridefinizione delle competenze del Settore Affari Generali e Legali nell’ambito della UOC Affari Generali e Legali – Provvedimenti conseguenti” con la quale è stata confermata l’attribuzione al settore Affari Generali afferente a detta Unità Operativa delle funzioni di privacy e accesso;
- n.372 del 28/12/2015, avente ad oggetto “Ridefinizione della struttura organizzativa delle Aree di attività amministrative territoriali, ospedaliere e di anticorruzione, trasparenza e privacy”, con la quale si è provveduto, tra l’altro, ad individuare la UO “Anticorruzione, Trasparenza e Privacy”;
- n.12 del 29.01.2016, avente ad oggetto “Provvedimenti conseguenti alla ridefinizione della struttura organizzativa delle aree di attività amministrative territoriali, ospedaliere e di anticorruzione, trasparenza e privacy di cui alla deliberazione n.372/2015”, con la quale si è tra l’altro conferito, con decorrenza dalla data del 1.2.2016, l’incarico di Direzione della Struttura Complessa UO “Anticorruzione, Trasparenza e Privacy” alla Dr.ssa Grazia Matarante, Dirigente Amministrativo a tempo indeterminato di questa Azienda USL con trasferimento delle funzioni Privacy dalla UO Affari Generali e Legali alla UO Anticorruzione, Trasparenza e Privacy;
- n.47 del 13 febbraio 2017 con la quale sono state attribuite le deleghe all’adozione di atti amministrativi ai dirigenti responsabili di articolazioni organizzative aziendali, tra le quali le deleghe all’adozione di specifici atti amministrativi al Direttore della UO Anticorruzione, Trasparenza e Privacy;

Vista la nota prot. n.66887 del 25 maggio 2018 con la quale è stato adottato il Registro delle attività di trattamento dell’Azienda USL di Bologna;

Richiamata la nota prot. n.61715 del 16 maggio 2018 con la quale, in conformità al GDPR sopra richiamato, è stata designata, in via temporanea, la dott.ssa Gian Carla Pedrazzi, quale Responsabile della Protezione dei dati personali a decorrere dal 25 maggio 2018 e fino alla conclusione delle procedure avviate per il conferimento dell’incarico di Responsabile della protezione dei dati (RPD o DPO);

Preso atto della Deliberazione n.220 del 29/06/2018, recante “Designazione del Responsabile della Protezione dei Dati (RPD) ai sensi dell’art.37 del Regolamento UE 2016/679”, con la quale la Dr.ssa Federica Banorri è stata designata, a decorrere dal 1 luglio 2018, Responsabile della Protezione dati (RPD) dell’Azienda USL di Bologna;

Considerato che il GDPR - con riferimento ai soggetti - disciplina espressamente, oltre al Responsabile della Protezione dei Dati (RPD) - Data Protection Officer (DPO), le figure del “ **titolare del trattamento**” e del “ **responsabile del trattamento**”, riferendosi con quest'ultima espressione ai soli soggetti esterni alla organizzazione che trattano dati personali per conto del titolare del trattamento, e delinea la categoria delle «persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare [...]» (art.4, n.10);

Preso atto che - in attuazione dell'art.39 del GDPR (“Compiti del responsabile della protezione dei dati”) - al DPO spettano le funzioni e i compiti di seguito riportati:

- informare e fornire 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;
- assicurare, in collaborazione con i referenti privacy, attività di informazione/consulenza ai responsabili del trattamento nonché ai dipendenti che, in qualità di autorizzati al trattamento, eseguono operazioni di trattamento dati;
- sorvegliare l'osservanza della normativa in materia di protezione dei dati personali e delle policy aziendali, comprese l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti, coordinando il gruppo dei referenti aziendali individuati dalle singole Aziende/Enti dell’area metropolitana;
- fornire, se richiesti, pareri anche scritti in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento;
- cooperare 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;
- supportare le strutture aziendali deputate alla tenuta del Registro delle attività di trattamento delle singole Aziende/Enti, al fine di uniformarne la predisposizione;
- garantire 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);
- promuovere iniziative congiunte tra le Aziende/Enti affinché 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;
- favorire 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;

Considerato inoltre che l'Autorità Garante per la protezione dei dati personali, a sua volta, nel Documento Guida all´applicazione del Regolamento europeo in materia di 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»;*

Rilevato che, ai sensi dell'art.32 del GDPR, al titolare del trattamento competono le decisioni atte a garantire il profilo di sicurezza del trattamento dei dati personali, « *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 ai sensi degli artt.29 e 32 del GDPR chiunque agisca sotto l'autorità del titolare del trattamento e abbia accesso a dati personali possa trattare tali dati solo se adeguatamente istruito;

Ritenuto, alla luce delle novità introdotte dal GDPR, dal D.Lgs. n.101/2018 e delle raccomandazioni del Garante per la protezione dei dati personali sopra richiamati, di:

- garantire, nel rispetto degli adempimenti previsti dalla normativa vigente, continuità in merito alle scelte organizzative in precedenza assunte dalla Azienda, in ordine ai livelli delle responsabilità e alla individuazione dei soggetti designati ad eseguire operazioni di trattamento;
- modificare parzialmente l'attuale organigramma delle responsabilità privacy aziendali, sia in termini di professionisti coinvolti, che di attribuzioni di compiti e funzioni;
- individuare le modalità di designazione di tali soggetti, utilizzando altresì la terminologia di cui al GDPR.

Valutata la necessità di istituire il Gruppo Aziendale Privacy (GAP), coordinato dal Direttore della UO Anticorruzione Trasparenza e Privacy, che, in attuazione dei principi di informazione e sensibilizzazione richiamati dal GDPR, ha il mandato di assicurare un presidio aziendale per quel che concerne gli adempimenti organizzativi e procedurali derivanti dalle nuove disposizioni normative in materia di protezione dei dati personali, composto dal:

- Direttore UO Tecnologie Informatiche e di Comunicazione o suo delegato;
- Direttore Sanitario di Presidio o suo delegato;
- Direttore del Dipartimento Cure Primarie o suo delegato;
- Direttore del Dipartimento di Sanità Pubblica o suo delegato;
- Direttore Direzione Assistenziale Tecnica e Riabilitativa o suo delegato;
- Direttore Operativo IRCCS o suo delegato
- Direttore Amministrativo o suo delegato.

Ritenuto di affidare al GAP i seguenti compiti:

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

Bologna, a seguito degli approfondimenti e delle analisi effettuate dal coordinatore del GAP con il DPO nel Tavolo di area metropolitana;

- supportare i Referenti privacy, nell'aggiornamento del Registro delle attività di trattamento di dati personali effettuati dalle strutture di appartenenza e nella eventuale valutazione di impatto;
- fornire supporto alle verifiche di sicurezza svolte dalla UO Tecnologie Informatiche e di Comunicazione e/o dal DPO;
- coordinare le richieste di parere al DPO da parte dei singoli Referenti Privacy ;
- effettuare la valutazione del rischio, a seguito dell'istruttoria effettuata su segnalazione di violazione, per fornire ogni utile elemento al Titolare del trattamento;

Valutato opportuno modificare l'attuale organigramma privacy ridefinendo contestualmente i profili di responsabilità nella gestione degli adempimenti connessi al trattamento dei dati;

Ritenuto di individuare quali Referenti privacy (già *Responsabili interni di trattamento*), in considerazione della natura gestionale e della complessità delle strutture organizzative in termini di attività di trattamento dati e di personale assegnato, solo coloro che - già individuati nella deliberazione n.267/2005 quali Responsabili di trattamento - ricoprano specificatamente gli incarichi di seguito indicati:

- Direttori di Unità Operativa Complessa (SC);
- Dirigenti Responsabili di Unità Operativa Semplice Dipartimentale (UOSD);
- Direttori di Programmi Gestionali.

Specificato che l'individuazione dei Referenti privacy avverrà, direttamente con la sottoscrizione del contratto individuale di lavoro;

Precisato che i compiti e le funzioni attribuiti in materia di protezione dei dati personali nonché le istruzioni operative in materia di trattamento dei dati personali, impartite dal Titolare del Trattamento ed allegate al presente provvedimento (allegati 1 e 2) sono pubblicate sulla intranet aziendale al link: https://intranet.internal.ausl.bologna.it/servizi/dg/uo-anticorruzione-trasparenza-e-privacy-sc/privacy-e-diritto-di-accesso,

Dato atto che i Responsabili interni di trattamento, ora Referenti privacy, mantengono le responsabilità in materia di trattamento dei dati personali;

Precisato inoltre che la individuazione di Referente privacy può rendersi necessaria anche per altri soggetti da individuarsi di volta in volta, in virtù delle particolarità organizzative e funzionali delle attività di competenza e/o della tipologia dei dati trattati;

Considerato che la individuazione di Referente privacy - in quanto connaturata all'attribuzione di uno o più degli incarichi sopra citati - si intende revocata di diritto alla cessazione dell'incarico medesimo;

Valutato che, al fine di conferire continuità alle suddette responsabilità in materia di trattamento di dati personali, la individuazione di Referente privacy si estende ai dirigenti che, in caso di vacanza del ruolo del Direttore o del Responsabile, assumano la relativa responsabilità ad interim;

Ritenuto opportuno fare salvi tutti gli effetti delle pregresse nomine a "responsabili [interni] del trattamento", d'ora in poi, "Referenti privacy", dichiarando tuttavia decadute le nomine non più compatibili con il nuovo assetto organizzativo;

Valutato di dare mandato alla UO Anticorruzione, Trasparenza e Privacy di aggiornare l'elenco dei "responsabili (interni) del trattamento dei dati", d'ora in poi denominati "Referenti privacy", elenco pubblicato nella intranet aziendale nell'apposita sezione dedicata, garantendo la rappresentazione corretta dei nominativi indicati, corrispondente alla nuova organizzazione ed alla terminologia ridefinita in linea con il GDPR, e monitorando nel tempo le modifiche, sia organizzative sia riguardanti la titolarità degli incarichi sopra menzionati;

Ritenuto altresì che per " *personale autorizzato al trattamento dei dati*" (già personale " *incaricato di trattamento dati"*) s'intende, in via generale, tutto il personale dipendente dell'Azienda, nonché tutti coloro che, pur in assenza di un rapporto di lavoro dipendente, siano, a vario titolo, inseriti stabilmente all'interno dell'organizzazione ed effettuino operazioni di trattamento dei dati, ognuno per il proprio specifico ambito di competenza professionale con riferimento ai dati afferenti alla U.O cui sono formalmente assegnati, come risultanti dal Registro delle attività di trattamento e dalle funzioni attribuite alla U.O. di appartenenza specificate nell'Atto aziendale, come previsto all'art.3 del D.Lgs. n.502/1992 e ss.mm. ed ii., nel relativo Regolamento attuativo e nelle successive deliberazioni di integrazione/modifica;

Preso atto che il personale già nominato incaricato di trattamento - alla data di adozione della presente deliberazione - sia da considerarsi personale autorizzato al trattamento, ai sensi dell'art.29 del GDPR e che tale personale potrà reperire le nuove istruzioni per il personale autorizzato sulla intranet aziendale al link: https://intranet.internal.ausl.bologna.it/servizi/dg/uo-anticorruzione-trasparenza-e-privacy-sc/privacy-e-diritto-di-accesso;

Preso atto che:

- per il personale che entrerà in servizio – successivamente alla data di adozione della presente deliberazione - sarà il Servizio Unico Metropolitano Amministrazione del Personale (SUMAP) a provvedere alla nomina di autorizzato ex art.29 GDPR al momento della sottoscrizione del contratto individuale di lavoro, del contratto di collaborazione coordinata e continuativa, del contratto libero professionale, del contratto di borsa di studio etc, e a fornire le istruzioni operative di carattere generale, di cui all'allegato 3, parte integrante e sostanziale della presente deliberazione;
- per i tirocinanti, frequentatori, specializzandi, medici in formazione specialistica sarà l'UO Formazione a provvedere alla nomina di autorizzato al trattamento e a fornire le istruzioni operative di carattere generale, di cui all'allegato 2, parte integrante e sostanziale della presente deliberazione;

- per i medici specialisti ambulatoriali ed i medici di emergenza territoriale (MET) che entreranno in servizio – successivamente alla data di adozione della presente deliberazione - sarà il Dipartimento Cure Primarie (DCP) a provvedere alla nomina di autorizzato ex art.29 GDPR al momento della sottoscrizione della convenzione/contratto, e a fornire le istruzioni operative di carattere generale, di cui all'allegato 2 , parte integrante e sostanziale della presente deliberazione;

Precisato che, per i trattamenti di dati effettuati con procedura informatizzata, l'attivazione delle credenziali di autenticazione informatica per il personale autorizzato resta in capo al Referente privacy (già responsabile interno di trattamento), il quale deve specificare a quali dati e tipi di operazioni ciascun autorizzato può accedere in relazione ai compiti assegnati e disporne tempestivamente la disattivazione in caso di variazione/cessazione dell'incarico;

Preso altresì atto che, più in generale, la mancata osservanza delle disposizioni, poste dalla normativa in materia di trattamento dei dati personali, per il Referente privacy e per il personale autorizzato, dà luogo a responsabilità disciplinare ai sensi dell'art.55 e ss. del D.Lgs. n.165/2001 e come prevista dal Codice di Comportamento di questa Azienda, approvato con Deliberazione n.166 del 29 maggio 2018, nonché dalle disposizioni dei vigenti CCNL della Dirigenza e del CCNL Comparto Sanità;

Precisato inoltre che, qualora l'Autorità di controllo applichi una sanzione al titolare di trattamento per mancato rispetto delle istruzioni operative da parte del Referente privacy o del personale autorizzato al trattamento, il Titolare del Trattamento si riserverà di valutare eventuali ed ulteriori azioni conseguenti;

Acquisito il parere favorevole della Dott.ssa Federica Banorri, in qualità di DPO;

Preso atto che dall'adozione del presente provvedimento non derivano oneri aggiuntivi a carico del bilancio dell'Azienda USL di Bologna;

Delibera

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

1) di prendere atto che il "sistema privacy" delineato dal GDPR e confermato a livello nazionale dal D.Lgs. n.196/2003, così come modificato dal D.lgs. n.101/2018, si caratterizza per un approccio di tipo sostanziale e proattivo e per un accrescimento delle responsabilità del titolare e di tutti i soggetti chiamati a trattare i dati personali all'interno dell'organizzazione aziendale;

2) di dare atto che il presente provvedimento, recependo le novità normative introdotte dal Legislatore europeo e nazionale, ridefinisce la organizzazione dei profili di responsabilità e la gestione degli adempimenti connessi al trattamento dei dati;

3) di dare atto della necessità di garantire continuità rispetto alle scelte organizzative assunte negli anni dalla Azienda USL di Bologna modificando parzialmente il preesistente organigramma delle responsabilità privacy aziendali adattandolo all'attuale assetto organizzativo aziendale;

4) di prendere atto che, in conformità al GDPR, le preesistenti figure dei "responsabili [interni] del trattamento", d'ora in poi, saranno definiti "Referenti privacy";

5) di individuare quali "Referenti privacy" (già Responsabili interni di trattamento), in considerazione della natura gestionale e della complessità delle strutture organizzative in termini di attività di trattamento dati e di personale assegnato, solo coloro che - già individuati nella deliberazione n.267/2005 quali Responsabili di trattamento - ricoprano specificatamente gli incarichi di seguito indicati:

- Direttori di Unità Operativa Complessa (SC);
- Dirigenti Responsabili di Unità Operativa Semplice Dipartimentale (UOSD);
- Direttori di Programmi Gestionali;

6) di attribuire ai Referenti privacy le funzioni dettagliate nel documento allegato 1 alla presente deliberazione ("Compiti, funzioni e poteri dei Referenti privacy");

7) di dare mandato al SUMAP di trasmettere la presente deliberazione ai Dirigenti attualmente titolari degli incarichi dirigenziali di cui al punto 5 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;

8) di specificare che non si provvederà quindi ad individuare i Referenti privacy mediante atto di designazione espresso, in quanto tale individuazione discende direttamente dal contratto individuale di lavoro sottoscritto all'atto dell'assunzione, con la precisazione che le istruzioni operative in materia di trattamento dei dati personali impartite dal Titolare del trattamento sono contenute in allegato alla presente deliberazione, quale parte integrante e sostanziale (allegato 1) e pubblicate sulla intranet aziendale al link: https://intranet.internal.ausl.bologna.it/servizi/dg/uo-anticorruzione-trasparenza-e-privacy-sc/privacy-e-diritto-di-accesso

9) di dare atto che i Responsabili interni di trattamento, ora individuati quali Referenti privacy, mantengono le responsabilità in materia di trattamento dei dati personali;

10) di precisare inoltre che la individuazione di Referente Privacy può rendersi necessaria anche per altri soggetti da individuarsi di volta in volta, in virtù delle particolarità organizzative e funzionali delle attività di competenza e/o della tipologia dei dati trattati;

11) di dare atto che la individuazione di Referente privacy - in quanto connaturata all'attribuzione di uno o più degli incarichi sopra citati - si intende revocata di diritto alla cessazione dell'incarico medesimo;

12) di specificare che, al fine di conferire continuità alle suddette responsabilità in materia di trattamento di dati personali, la individuazione di Referente privacy si estende ai dirigenti che, in caso di vacanza del ruolo del Direttore o del Responsabile, assumano la relativa responsabilità ad interim;

13) di fare salvi tutti gli effetti delle pregresse nomine a "responsabili [interni] del trattamento", d'ora in poi, "Referenti Privacy", dichiarando tuttavia decadute le nomine non più compatibili con il nuovo assetto organizzativo;

14) di dare mandato al SUMAP di comunicare le variazioni di attribuzione degli incarichi, di cui al punto 5, alla UO Anticorruzione, Trasparenza e Privacy che provvederà ad aggiornare l'elenco dei "responsabili (interni) del trattamento dei dati", d'ora in poi denominati "Referenti privacy", pubblicato sulla intranet all'interno dell'apposita sezione dedicata, garantendo la rappresentazione corretta dei nominativi indicati, corrispondente alla nuova organizzazione ed alla terminologia ridefinita in linea con il GDPR e monitorando nel tempo le modifiche, sia organizzative sia riguardanti la titolarità degli incarichi sopra menzionati;

15) di precisare che per "personale autorizzato al trattamento dei dati" (già personale incaricato di trattamento dati) s'intende, in via generale, tutto il personale dipendente dell'Azienda, nonché tutti coloro che, pur in assenza di un rapporto di lavoro dipendente, siano, a vario titolo, inseriti stabilmente all'interno dell'organizzazione ed effettuino operazioni di trattamento dei dati personali, ognuno per il proprio specifico ambito di competenza professionale;

16) di precisare altresì che il personale già nominato incaricato di trattamento - alla data di adozione della presente deliberazione - sia da considerarsi personale autorizzato al trattamento, ai sensi dell'art.29 del GDPR;

17) 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 ad integrare e dettagliare tale schema, se necessario, in base alle caratteristiche specifiche dei singoli trattamenti o in base alle specifiche mansioni dei soggetti autorizzati;

18) di comunicare l'autorizzazione al trattamento a tutti i dipendenti ed alle categorie di personale elencate al precedente punto 13 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 policy"; dando mandato al Servizio Unico Metropolitano Amministrazione del Personale, alla UO Sviluppo organizzativo, Professionale e Formazione e al Dipartimento delle Cure Primarie, secondo le rispettive competenze, di procedere analogamente nei confronti del personale di nuova "assunzione", integrando altresì i (futuri) contratti di lavoro con apposita clausola;

19) di precisare che per i trattamenti di dati effettuati con procedura informatizzata, l'attivazione delle credenziali di autenticazione informatica per il personale autorizzato resta in capo al Soggetto Referente Privacy Aziendale (già responsabile interno di trattamento) il quale deve specificare a quali dati e tipi di operazioni ciascun autorizzato può accedere in relazione ai propri compiti e disporne tempestivamente la disattivazione in caso di variazione/cessazione dell'incarico;

20) di prendere altresì atto che, più in generale, la mancata osservanza delle disposizioni poste dalla normativa in materia di trattamento dei dati personali per il personale referente privacy aziendale e per il personale autorizzato dà luogo a responsabilità disciplinare, ai sensi dell'art. 55 e ss. del D.Lgs. n.165/2001, come previsto altresì dal Codice di Comportamento di questa Azienda, approvato con Deliberazione n.166 del 29 maggio 2018, nonché dalle disposizioni dei vigenti CCNL della Dirigenza e del CCNL Comparto Sanità;

21) di precisare inoltre che, qualora l'Autorità di controllo applichi una sanzione al titolare di trattamento per mancato rispetto delle istruzioni operative da parte del Referente privacy o del personale autorizzato al trattamento, il Titolare del Trattamento si riserverà di valutare eventuali ed ulteriori azioni conseguenti;

22) di istituire il Gruppo Aziendale Privacy (GAP), coordinato dalla UO Anticorruzione Trasparenza e Privacy, in attuazione dei principi di informazione e sensibilizzazione richiamati dal GDPR, con il mandato di assicurare un presidio aziendale per quel che concerne gli adempimenti organizzativi e procedurali derivanti dalle nuove disposizioni normative in materia di protezione dei dati personali, composto da:

- Direttore UO Tecnologie Informatiche e di Comunicazione o suo delegato;
- Direttore Sanitario di Presidio o suo delegato;
- Direttore del Dipartimento Cure Primarie o suo delegato;
- Direttore del Dipartimento di Sanità Pubblica o suo delegato;
- Direttore Direzione Assistenziale Tecnica e Riabilitativa o suo delegato;
- Direttore Operativo IRCCS o suo delegato;
- Direttore Amministrativo o suo delegato;

23) di affidare al GAP i seguenti compiti:

- supportare i Referenti privacy nell'adozione delle misure adeguate ed efficaci per la tutela della riservatezza, integrità e disponibilità del patrimonio informativo come individuate dall'Azienda USL di Bologna, a seguito degli approfondimenti e delle analisi effettuate dal coordinatore del GAP con il DPO nel Tavolo di area metropolitana;
- supportare i Referenti privacy, nell'aggiornamento del Registro delle attività di trattamento di dati personali effettuate dalle strutture di appartenenza e nella eventuale valutazione di impatto;
- fornire supporto alle verifiche di sicurezza svolte dalla UO Tecnologie Informatiche e di Comunicazione e/o dal DPO;
- coordinare le richieste di parere al DPO da parte dei singoli Referenti privacy;
- effettuare la valutazione del rischio a seguito dell'istruttoria effettuata, su segnalazione di violazione, per fornire ogni utile elemento al Titolare del trattamento;

24) di dare atto che il presente provvedimento sostituisce integralmente la deliberazione aziendale n.267/2005 “Determinazioni in merito agli adempimenti di cui al D.lgs. n.196/2003 Codice in materia di protezione dei dati personali”;

25) di prendere atto che dall’adozione del presente provvedimento non derivano oneri aggiuntivi a carico del bilancio dell’Azienda USL di Bologna;

26) di specificare che il Responsabile del Procedimento ai sensi della legge n.241/1990 e ss. mm. ed ii. è la Dr.ssa Grazia Matarante, Dirigente Amministrativo a tempo indeterminato, Direttore della UO Anticorruzione, Trasparenza e Privacy;

27) di trasmettere copia del presente provvedimento a:

- Direttori di Dipartimenti di Produzione Ospedaliera e Territoriale;
- Direttore Scientifico IRCCS;
- Direttore Operativo IRCCS;
- Direttore UO Amministrativa IRCCS;
- Direttore Dipartimento Amministrativo;
- Direttori di UO del Dipartimento Amministrativo;
- Direttore Dipartimento Tecnico Patrimoniale;
- Direttore Dipartimento Farmaceutico;
- DAAT – Dipartimento Attività Amministrative Territoriali;
- Direttori UO Staff specifico del DG-DS-DA;
- Direttori UO Staff di Direzione aziendale;
- Direttori di Distretto;
- DATeR – Direzione Assistenziale Tecnica e Riabilitativa
- Direttore UO Amministrativa DCP;
- Direttore UO Amministrativa DSM;
- Direttore UO Amministrativa DSP;
- Direttore UO Amministrativa DATeR
- Responsabile della Protezione Dati
- Collegio Sindacale.

Responsabile del procedimento ai sensi della L. 241/90:
Grazia Matarante

Allegato 1

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 (RGPD o GDPR) e del D.Lgs. n.196/2003, come modificato dal D.Lgs. n.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 della UO Anticorruzione, Trasparenza e Privacy, del Gruppo Aziendale Privacy (GAP) e della UO Tecnologia Informatiche e di Comunicazione (es. regolamento aziendale sull'utilizzo delle risorse informatiche, linee di indirizzo per la gestione del Dossier Sanitario Elettronico, procedura per la gestione della violazione dei dati personali o data breach, etc.);
    b) le istruzioni di carattere generale impartite dal Titolare a tutti i soggetti autorizzati al trattamento dei dati personali (di cui all'**allegato 2**);
    c) eventuali ulteriori specifiche istruzioni, predisposte dal Titolare o dai Referenti privacy, 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, etc.), 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 USL di Bologna ed assicurare la partecipazione dei propri autorizzati;
- Fornire le informazioni richieste dalla UO Anticorruzione, Trasparenza e Privacy e dal Gruppo Aziendale Privacy (GAP), segnalare ogni questione rilevante in materia e trasmettere tempestivamente istanze e reclami degli interessati, da far pervenire al DPO;
- Comunicare alla UO Anticorruzione, Trasparenza e Privacy e al Gruppo Aziendale Privacy (GAP) 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 delle attività di trattamento aziendale;
- Collaborare con la UO Anticorruzione, Trasparenza e Privacy e con il Gruppo Aziendale Privacy (GAP) 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 personali 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 alla UO Anticorruzione, Trasparenza e Privacy, anche ai fini dell’aggiornamento del Registro delle attività di trattamento dei dati aziendale;
- Comunicare tempestivamente alla UO Anticorruzione, Trasparenza e Privacy e al Gruppo Aziendale Privacy (GAP) 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. dati 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 dal 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 da 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 devono essere fornite le informazioni 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 idonei 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 contenenti dati riferiti alla salute. A tal specifico fine si rinvia alle disposizioni aziendali (deliberazione n.60 del 24 aprile 2007, recante Regolamento per l'utilizzo della Posta Elettronica e di Internet, e ss.mm. ii.);
- 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, occorrerà 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 (es. un armadio o un cassetto chiusi a chiave, una cassaforte, etc.);

Per il Regolamento aziendale per l'utilizzo delle risorse informatiche dell'Azienda USL di Bologna si rinvia all'allegato alla deliberazione aziendale n.460 del 28 dicembre 2017 (e ss.mm. ed ii.).

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 si 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 USL di Bologna.

Le suddette istruzioni di carattere generale 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 a cui si rinvia, reperibili alla pagina intranet dedicata *https://intranet.internal.ausl.bologna.it/servizi/dg/uo-anticorruzione-trasparenza-e-privacy-sc/privacy-e-diritto-di-accesso*

Allegato 3

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/la sottoscritto/a _____

(indicare il nome del Referente Privacy di afferenza)

in qualità di Referente Privacy di UOC/UOSD/Programma _____

_____

DESIGNA

(indicare NOME e COGNOME)

in qualità di ……

(indicare funzione, ruolo,…)

SOGGETTO AUTORIZZATO AL TRATTAMENTO DEI DATI PERSONALI 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 dedicata della rete intranet aziendale (https://intranet.internal.ausl.bologna.it/servizi/dg/uo-anticorruzione-trasparenza-e-privacy-sc/privacy-e-diritto-di-accesso), delle prescrizioni di carattere specifico e delle 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 (username 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 dati e informazioni a soggetti terzi (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 istruzioni di carattere specifico e 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 Referente privacy 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 soprariportate, le istruzioni di carattere generale impartite dal Titolare, allegate al presente atto di designazione e disponibili nella sezione dedicata della rete intranet aziendale, e le eventuali istruzioni di carattere specifico che Le verranno eventualmente impartite per l'ambito di competenza e per il profilo professionale di appartenenza.

È fatto obbligo a ciascun professionista autorizzato al trattamento di 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 personali nello 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 di lavoro con l'Azienda USL di Bologna e viene a cessare al modificarsi del rapporto di lavoro o a seguito di esplicita revoca dello stesso.

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

Il/la sottoscritto/a _____

(indicare NOME e COGNOME)

DICHIARA

1. di aver ricevuto la designazione ad autorizzato al trattamento dei dati personali;
2. di aver attentamente letto e compreso il contenuto del presente atto e del suo allegato, e di impegnarsi ad osservare tutte le istruzioni impartite;
3. di obbligarsi ad osservare le ulteriori direttive/regolamentazioni aziendali reperibili alla sezione intranet dedicata (https://intranet.internal.ausl.bologna.it/servizi/dg/uo-anticorruzione-trasparenza-e-privacy-sc/privacy-e-diritto-di-accesso)
4. di prendere atto che l'obbligo di riservatezza correlato all'incarico va osservato anche successivamente alla conclusione dello stesso.

Data _____

Firma _____

Allegato

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. dati 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 dal 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 da 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 devono essere fornite le informazioni 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 idonei 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 contenenti dati riferiti alla salute. A tal specifico fine si rinvia alle disposizioni aziendali (deliberazione n.60 del 24 aprile 2007, recante Regolamento per l'utilizzo della Posta Elettronica e di Internet, e ss.mm. ed ii.);
- 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, occorrerà 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 (es. un armadio o un cassetto chiusi a chiave, una cassaforte, etc.);

Per il Regolamento aziendale per l'utilizzo delle risorse informatiche dell'Azienda USL di Bologna si rinvia all'allegato alla deliberazione aziendale n.460 del 28 dicembre 2017 (e ss.mm. ed ii.).

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 si 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 USL di Bologna.

Le suddette istruzioni di carattere generale 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 a cui si rinvia, reperibili alla pagina intranet dedicata *https://intranet.internal.ausl.bologna.it/servizi/dg/uo-anticorruzione-trasparenza-e-privacy-sc/privacy-e-diritto-di-accesso*

~~*1. Regolamento per il corretto utilizzo dei sistemi informatici aziendali;*~~
~~*2. Regolamento sul Dossier Sanitario elettronico;*~~
~~*3. ……;*~~
~~*4. ……*~~