



**ATTO DI DESIGNAZIONE A
RESPONSABILE/DELEGATO AL TRATTAMENTO DEI DATI PERSONALI
Art. 28, Regolamento (UE) 2016/679**

Considerato che:

- con atto dirigenziale del Servizio n. del, a seguito di (es: gara a procedura ristretta), tra l'AOU di Modena e la Ditta è stato stipulato/rinnovato/ecc. il contratto/convenzione per; nella esecuzione del suddetto rapporto convenzionale e nel compimento degli atti conseguenti, la suddetta Ditta compie necessariamente operazioni di trattamento di dati personali per conto dell'AOU di Modena/Titolare del trattamento; l'ambito del trattamento e i dati che ne sono oggetto sono meglio specificati nell'Allegato 1 al presente Atto "Ambito del trattamento";
- il Regolamento Generale (UE) 2016/679 sulla protezione dei dati personali (di seguito anche GDPR o Regolamento), definitivamente applicabile in Italia dal 25 maggio 2018, dispone che qualora un trattamento debba essere effettuato per conto del Titolare, quest'ultimo ricorre unicamente a responsabili del trattamento che garantiscano la adozione di misure tecniche ed organizzative adeguate, in modo tale che il trattamento sia conforme alla normativa in materia di protezione dati e garantisca la tutela dei diritti dell'interessato;
- per l'ambito di attribuzioni, funzioni e competenze conferite, codesta ditta possiede i requisiti di esperienza, capacità e affidabilità idonei a garantire il pieno rispetto delle vigenti disposizioni in materia di trattamento dei dati, ivi compreso il profilo relativo alla sicurezza.

Tutto ciò premesso, al fine di provvedere alla corretta gestione degli adempimenti previsti dal GDPR, tra le parti si conviene e si stipula quanto segue

Designazione del Responsabile del trattamento

Con il presente atto il direttore generale, legale rappresentante dell'AOU di Modena/Titolare del trattamento nomina la codesta rispettabile ditta responsabile del trattamento dei dati personali, per quanto sia necessario alla corretta esecuzione del rapporto convenzionale indicato in premessa.

Obblighi e compiti del Responsabile del trattamento

Codesta ditta, responsabile del trattamento tratta i dati personali per conto del Titolare del trattamento solo ed esclusivamente ai fini della esecuzione dei servizi oggetto del

contratto/convenzione, nel rispetto della normativa vigente in materia di protezione dei dati personali, nonché delle istruzioni impartite dal Titolare nel presente Atto o in atti successivi.

Ogni trattamento di dati personali da parte del Responsabile del trattamento deve avvenire nel rispetto dei principi, dei limiti e delle modalità di cui all'art. 5 del GDPR.

Il Responsabile del trattamento, operando nell'ambito dei suddetti principi, deve attenersi ai seguenti compiti, con riferimento rispettivamente a:

persone preposte allo svolgimento di operazioni di trattamento sui dati personali:

sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, designa espressamente e per iscritto i dipendenti e i collaboratori autorizzati/incaricati allo svolgimento di operazioni di trattamento sui dati personali oggetto del contratto, attribuendo loro specifici compiti e funzioni ed impartendo adeguate informazioni ed istruzioni;

Al fine di garantire un trattamento corretto, lecito e sicuro si adopera per rendere effettive le suddette istruzioni, curando la formazione di tali soggetti - sia in tema di protezione dei dati personali che, ove occorra, di sicurezza informatica - vigilando sul loro operato, vincolandoli alla riservatezza su tutte le informazioni acquisite nello svolgimento delle loro attività, anche successivamente alla cessazione del rapporto di lavoro/collaborazione con la Ditta stessa;

comunica al Titolare del trattamento su specifica richiesta l'elenco aggiornato dei dipendenti/collaboratori autorizzati al trattamento, nonché qualsiasi variazione dei profili autorizzativi concessi a tali persone per motivi di sicurezza;

registro delle attività di trattamento:

ove ne sia tenuto, identifica e censisce i trattamenti di dati personali, le banche dati e gli archivi gestiti con supporti informatici e/o cartacei necessari all'espletamento delle attività oggetto della Convenzione al fine di predisporre il registro delle attività di trattamento svolte per conto della Azienda AOU di Modena/Titolare da esibire in caso di ispezione della Autorità Garante e contenente almeno le seguenti informazioni:

- il nome e i dati di contatto del Responsabile, del Titolare del trattamento per conto del quale il Responsabile agisce e, ove applicabile, del Responsabile della protezione dei dati;
- le categorie dei trattamenti effettuati per conto del Titolare;
- se del caso, i trasferimenti di dati personali verso paesi terzi, compresa l'identificazione del paese terzo e la relativa documentazione di garanzia;
- la descrizione generale delle misure di sicurezza tecniche ed organizzative applicate a protezione dei dati;

obblighi di sicurezza:

- adotta le misure tecniche e organizzative adeguate per proteggere la sicurezza, la riservatezza e l'integrità dei dati personali tenendo conto dei rischi di varia probabilità e gravità (di distruzione o perdita, di modifica, di divulgazione non autorizzata o di accesso accidentale o illegale a dati trasmessi, conservati o comunque trattati), dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento;
- definisce una politica di sicurezza per assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e servizi afferenti il trattamento dei dati; le modalità per garantire tali livelli di sicurezza dovranno essere comunicate al titolare nel caso di esplicita richiesta;

- si impegna ad utilizzare strumenti, applicazioni e/o servizi che rispettino i principi di protezione dei dati personali fin dalla progettazione (privacy by design) e per impostazione predefinita (privacy by default).
- assicura la capacità di ripristinare tempestivamente la disponibilità e l'accesso ai dati in caso di incidente fisico o tecnico;
- definisce una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche ed organizzative applicate;
- ulteriori misure di sicurezza sono individuate in relazione allo specifico trattamento di dati da parte del fornitore.

“Data Breach”:

comunica al Titolare del trattamento, senza ingiustificato ritardo dopo esserne venuto a conoscenza - e comunque entro 12 ore - qualsiasi evento che possa comportare una violazione, anche accidentale, dei dati personali oggetto di trattamento, fornendo tutte le informazioni disponibili sull'evento e prestando la necessaria collaborazione al Titolare in relazione all'adempimento degli obblighi sullo stesso gravanti di notifica delle suddette violazioni alla Autorità Garante e/o di comunicazione delle stesse agli interessati; a tal fine il responsabile porrà in essere per quanto compatibile con il contesto e la natura della violazione, la procedura predisposta dal Titolare del trattamento, prendendone visione nella sezione Privacy del sito internet dell'Azienda: <http://www.aou.mo.it/privacy>.

valutazione di impatto:

fornisce tutte le informazioni e tutti gli elementi utili al Titolare per la effettuazione, da parte di quest'ultimo, della valutazione di impatto sulla protezione dei dati, nonché della eventuale consultazione preventiva alla Autorità Garante ai sensi degli artt. 35 e 36 del GDPR;

amministratori di sistema (se necessario in base al servizio/fornitura):

conformemente al Provvedimento della Autorità Garante del 27 novembre 2008 e sim, in tema di amministratori di sistema, si impegna a:

- designare quali amministratori di sistema le figure professionali dedicate alla gestione e alla manutenzione di impianti di elaborazione o di loro componenti con cui vengono effettuati trattamenti di dati personali;
- predisporre e conservare l'elenco contenente gli estremi identificativi delle persone fisiche qualificate quali amministratori di sistema e le funzioni ad essi attribuite;
- comunicare almeno annualmente al Titolare l'elenco aggiornato degli amministratori dei sistemi;
- verificare annualmente l'operato degli amministratori di sistema, informando il Titolare circa le risultanze di tale verifica;
- mantenere i file di log previsti in conformità a quanto previsto nel suddetto provvedimento.

istanze degli interessati:

- collabora con il Titolare per fornire tempestivamente tutte le informazioni necessarie e/o i documenti utili al fine di soddisfare l'obbligo del Titolare del trattamento di dare seguito alle

richieste degli interessati di cui al Capo III del GDPR (ad es.: esercizio dei diritti di accesso, rettifica, limitazione, opposizione al trattamento dei dati);

- collabora con il *Data Protection Officer* (DPO) del titolare del trattamento, provvedendo a fornire ogni informazione dal medesimo richiesta;
- qualora il trattamento dei dati personali oggetto della Convenzione comporti la raccolta di dati personali da parte del Responsabile del trattamento, questi provvede al rilascio della relativa informativa ai soggetti interessati.
- Il Responsabile affigge inoltre i cartelli contenenti l'informativa in tutti i luoghi ad accesso pubblico, con la precisazione che l'informazione resa attraverso la cartellonistica integra, ma non sostituisce l'obbligo di informativa in forma orale o scritta;

rapporti con le Autorità:

provvede ad informare immediatamente il Titolare del trattamento di ogni richiesta, ordine ovvero attività di controllo da parte dell'Autorità Garante per la protezione dei dati personali o dell'Autorità Giudiziaria e coadiuva il Titolare stesso nella difesa in caso di procedimenti dinanzi alle suddette Autorità che riguardino il trattamento dei dati oggetto del Convenzione;

ulteriori obblighi:

- mette a disposizione del Titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui alla normativa in materia di protezione dei dati personali e/o delle istruzioni del Titolare di cui al presente Atto di designazione e consente al Titolare del trattamento l'esercizio del potere di controllo e ispezione, prestando ogni ragionevole collaborazione alle attività di audit effettuate dal Titolare stesso o da un altro soggetto da questi incaricato o autorizzato, con lo scopo di controllare l'adempimento degli obblighi e delle istruzioni di cui al presente atto. Resta inteso che qualsiasi verifica condotta ai sensi del presente comma dovrà essere eseguita in maniera tale da non interferire con il normale corso delle attività del Responsabile e fornendo a quest'ultimo un ragionevole preavviso;

• si impegna altresì a:

- effettuare almeno annualmente un rendiconto in ordine all'esecuzione delle istruzioni ricevute dal Titolare (e agli adempimenti eseguiti) ed alle conseguenti risultanze;
- collaborare, se richiesto dal Titolare, con gli altri Responsabili del trattamento, al fine di armonizzare e coordinare l'intero processo di trattamento dei Dati Personali;
- realizzare quant'altro sia ragionevolmente utile e/o necessario al fine di garantire l'adempimento degli obblighi previsti dalla normativa applicabile in materia di protezione dei dati, nei limiti dei compiti affidati con il presente Atto di designazione;
- informare prontamente il Titolare di ogni questione rilevante ai fini di legge; a titolo esemplificativo e non esaustivo, nei casi in cui abbia notizia, in qualsiasi modo, che il trattamento dei dati personali violi la normativa in materia di protezione dei dati personali o presenti comunque rischi specifici per i diritti, le libertà fondamentali e/o la dignità dell'interessato o qualora, a suo parere, un'istruzione violi la normativa, nazionale o comunitaria, relativa alla protezione dei dati oppure qualora il Responsabile sia soggetto ad obblighi di legge che gli rendono illecito o impossibile agire secondo le istruzioni ricevute dal Titolare e/o conformarsi alla normativa o a provvedimenti dell'Autorità di Controllo.

Come sancito dal GDPR, qualora il Responsabile del trattamento determini autonomamente le finalità e i mezzi di trattamento in violazione del GDPR medesimo, sarà considerato Titolare del trattamento, assumendone i conseguenti oneri, rischi e responsabilità;

trasferimento di dati all'estero (se necessario in base al fornitore che si sta nominando):

altri Responsabili (Sub–responsabili):

per l'esecuzione di specifiche attività di trattamento per conto del Titolare e solamente previa autorizzazione scritta, specifica o generale del titolare stesso, il Responsabile del trattamento può ricorrere ad altro responsabile (c.d. Sub-responsabile del trattamento); quando ciò avvenga il Responsabile del trattamento si obbliga ad imporre per iscritto a tale Sub-responsabile, mediante atto giuridico vincolante, gli stessi obblighi in materia di protezione dei dati personali cui è soggetto il Responsabile stesso, in particolare in relazione agli obblighi in materia di sicurezza. In particolare, nel caso in cui il Responsabile del trattamento ricorra a un Sub-responsabile stabilito in un Paese extra-UE, sarà suo onere adottare adeguati strumenti per legittimare il trasferimento ai sensi degli artt. 44 e ss. del Regolamento. Il Titolare ha il diritto di chiedere al Responsabile del trattamento:

- il rilascio di copia degli accordi stipulati tra Responsabile e Sub-responsabile (omettendo le sole informazioni strettamente confidenziali e gli accordi economici, se del caso);
- di sottoporre ad audit i propri Sub-responsabili o comunque fornire conferma che tale audit siano stati condotti per dimostrare la conformità dei Sub-responsabili alla normativa in materia di protezione dei dati personali, nonché agli obblighi di cui al presente Atto.

Il Responsabile del trattamento si impegna espressamente ad informare il Titolare di eventuali modifiche riguardanti l'aggiunta o la sostituzione di eventuali Sub-responsabili del trattamento, dandogli così l'opportunità di opporsi a tali modifiche. Il Responsabile non può ricorrere ai Sub-responsabili nei cui confronti il Titolare abbia manifestato la sua opposizione.

Qualora il Sub-responsabile ometta di adempiere ai propri obblighi, il Responsabile del trattamento conserva nei confronti del Titolare del trattamento l'intera responsabilità dell'inadempimento degli obblighi del Sub-responsabile.

responsabile della protezione dei dati:

Il Responsabile del trattamento comunica al Titolare del trattamento il nome e i dati di contatto del proprio responsabile della protezione dei dati, ove designato.

Condizioni della nomina

Chiunque subisca un danno materiale o immateriale causato da una violazione della normativa in materia di protezione dati ha il diritto di ottenere il risarcimento del danno dal Titolare o dal Responsabile. In particolare, il Responsabile risponde per tale danno (anche per eventuali suoi Sub-responsabili) se non ha adempiuto agli obblighi che la normativa pone direttamente in capo ai responsabili o ha agito in modo difforme o contrario rispetto alle istruzioni impartite dal Titolare nel presente Atto o ad ulteriori istruzioni eventualmente trasmesse per iscritto dal Titolare.

In caso di richieste di risarcimento pervenute al Titolare, per violazioni compiute dal Responsabile, il Titolare si riserva il diritto di rivalsa nei confronti del Responsabile stesso.

Per quanto riguarda le sanzioni imputabili da parte dell'Autorità Garante, fanno fede gli art. 82, 83 e 84 del Regolamento (UE).

Resta fermo, in ogni caso, che la responsabilità penale per l'eventuale uso non corretto dei dati oggetto di tutela è a carico della singola persona cui l'uso illegittimo sia imputabile.

Resta inteso inoltre che la presente designazione non comporta alcun diritto per il Responsabile a uno specifico compenso, indennità o rimborso per l'attività svolta in qualità di Responsabile, ulteriore rispetto a quanto già previsto nel/nei contratti stipulati con il Titolare, indicati al presente Atto.

Durata del trattamento

Il presente Atto di designazione decorre dalla data in cui viene sottoscritto dalle parti ed è condizionato, per oggetto e per durata, al rapporto contrattuale/ convenzionale in corso tra AOU di Modena e codesta ditta e si intenderà revocato di diritto alla scadenza del rapporto o alla risoluzione, per qualsiasi causa, dello stesso.

La nomina si intende comunque estesa ad eventuali future proroghe e/o rinnovi di contratti, aventi ad oggetto le medesime o ulteriori attività che comportino un trattamento di dati personali analoghi da parte di codesta ditta in nome e per conto del Titolare AOU di Modena.

Resta fermo che, anche successivamente alla cessazione o alla revoca del contratto/convenzione, il Responsabile dovrà mantenere la massima riservatezza sui dati e le informazioni relative al Titolare delle quali sia venuto a conoscenza nell'adempimento delle sue obbligazioni.

Restituzione e cancellazione dei dati

Al termine del periodo di conservazione o all'atto della conclusione o della revoca del contratto, su richiesta, o in qualsiasi altro momento per sopravvenute necessità, la codesta ditta dovrà interrompere ogni operazione di trattamento dei dati personali e dovrà provvedere, a scelta del Titolare, all'immediata restituzione dei dati allo stesso, comprese tutte le eventuali copie di backup e tutta la documentazione cartacea, oppure alla loro integrale cancellazione, in entrambi i casi rilasciando contestualmente attestazione scritta che presso il Responsabile del trattamento non ne esista alcuna copia.

In caso di richiesta scritta del Titolare, il Responsabile è tenuto a indicare le modalità tecniche e le procedure utilizzate per la cancellazione/distruzione.

Per quanto non espressamente previsto nel presente Atto di designazione, si rinvia alle disposizioni generali vigenti in materia di protezione di dati personali, nonché alle disposizioni di cui al contratto/convenzione stipulato tra le parti, sopra individuato.

ALLEGATO 1 Ambito del trattamento (art. 28, paragrafo 3, GDPR)

Il presente Allegato costituisce parte integrante dell'Atto di designazione della codesta ditta quale Responsabile del trattamento da parte del Titolare/Azienda Ospedaliero-Universitaria di Modena e definisce in particolare:

Finalità del Trattamento

(Il presente elenco è da considerarsi a titolo puramente esemplificativo e non esaustivo)

Erogazione di prestazioni sanitarie

Finalità amministrative connesse alla cura dei pazienti (es.: accettazione, prenotazione, pagamento ticket.)

Fornitura di beni e/o servizi

Marketing

Profilazione

Erogazione di servizi di manutenzione IT

Altro (specificare) _____

Altro (specificare) _____

Altro (specificare) _____

Categorie degli interessati

(Il presente elenco è da considerarsi a titolo puramente esemplificativo e non esaustivo)

Pazienti

Dipendenti, specialisti convenzionati, universitari integrati, personale in formazione e altri collaboratori

Clienti

Consulenti

Fornitori

Altro (specificare) _____

Altro (specificare) _____

Tipologie di Dati personali da trattare

(Il presente elenco è da considerarsi a titolo puramente esemplificativo e non esaustivo)

dati anagrafici di pazienti

dati anagrafici di dipendenti, specialisti convenzionati, universitari integrati, personale in formazione e altri collaboratori

dati anagrafici di familiari, se presenti detrazioni di figli/coniuge a carico e assegni nucleo familiare

dati relativi allo stato di salute dei pazienti

o dati relativi allo stato di salute di dipendenti, specialisti convenzionati, universitari integrati, personale in formazione e altri collaboratori (disabilità, certificati medici, certificati di gravidanza)

dati genetici

dati biometrici

permessi di soggiorno

dati retributivi

dati anagrafici dei fornitori

abitudini di consumo

Altri dati (specificare) _____

ALLEGATO 2 Misure di sicurezza (art. 32, GDPR)

Misure di Sicurezza per Responsabili del Trattamento Dati che facciano accesso ai sistemi informativi e ai dispositivi dell'AOU di Modena

Definizioni/acronimi:

- AOU: Azienda Ospedaliero-Universitaria di Modena/Titolare del trattamento
- RET: Responsabile (Esterno) al Trattamento
- ICT: Information e Communication Technology (Tecnologie Informatiche e Telematiche)
- SUIC: Servizio Unico Ingegneria Clinica

1. Introduzione

Il presente documento descrive le misure tecniche e organizzative specifiche che l'Azienda Ospedaliero-Universitaria di Modena (AOU) richiede a soggetti che, a seguito di contratto di designazione a Responsabile (Esterno) al Trattamento Dati (RET), siano abilitati all'accesso ai sistemi informativi di AOU.

Le misure descritte nel presente documento sono da intendersi integrative rispetto a quanto previsto dalle normative vigenti in merito a trattamento dati personali e tutela del patrimonio, che rimangono pertanto il riferimento normativo principale a cui attenersi.

1.1. Principi Generali

In merito al trattamento dei dati personali, il RET si impegna ad una condotta orientata alla riservatezza, alla pertinenza e non eccedenza nel trattamento dati, adottando ovunque possibile metodologie e soluzioni tecniche che privilegino il trattamento di dati con formati non riconducibili all'interessato (es. anonimizzati, pseudonimizzati, ecc.).

In merito al trattamento di dati non personali, ma che costituiscono patrimonio aziendale, il RET si impegna ad una condotta rispettosa della proprietà del dato, consapevole del fatto che l'uso per altre finalità, la diffusione o la trasmissione a terzi di tali dati possono costituire

illecito penale, pertanto perseguibile, e che l'alterazione di dati può costituire danno per l'azienda.

1.2. Operatori del RET

Il RET si impegna a informare delle presenti misure e delle normative applicabili tutti gli operatori che siano coinvolti nel trattamento dati (con qualsiasi tipo di rapporto).

Il RET si impegna a censire tutti gli operatori coinvolti nel trattamento e, su richiesta, a fornire l'elenco con descrizione dei ruoli ad AOU.

Qualora il RET, nell'ambito del trattamento, si avvalsesse di credenziali con privilegi di amministrazione di sistema, è tenuto alla tenuta di un registro di tali operatori. Il RET si impegna, a fornire l'elenco con descrizione dei ruoli ad AOU.

Il RET deve definire formalmente un regolamento sull'utilizzo degli strumenti ICT oggetto del trattamento di dati di AOU. Tale regolamento deve essere conforme alla normativa vigente e garantire le misure minime organizzative atte a tutelare il dato di AOU. Tale regolamento deve essere, su richiesta, fornito ad AOU.

2. Servizi di Assistenza, Manutenzione, Supporto, Collaborazione, Erogazione di Servizi per Conto, che prevedano accesso ai sistemi di AOU

Quanto descritto nella presente sezione si applica a RET il cui rapporto con AOU preveda l'accesso ai sistemi informativi per l'erogazione di servizi di assistenza, manutenzione, supporto, collaborazione e erogazione per conto, di qualsiasi di tipo.

1. L'accesso ai sistemi AOU deve avvenire esclusivamente con modalità sicure, concordate con AOU. E' fatto divieto di adottare sistemi di collegamento e comunicazione non concordati con AOU.

2. L'accesso ai sistemi AOU deve avvenire a seguito di emissione di credenziali AOU, che sono personali e non condivisibili; la persona fisica associata alle credenziali sarà ritenuta responsabile, insieme al RET, di ogni azione svolta con tali credenziali e ritenuta responsabile di eventuali usi impropri (es. condivisione delle credenziali con colleghi).

- Eccezioni all'abbinamento nominale delle credenziali aziendali possono essere valutate dal Servizio ICT o SUIC solo in contesti tecnici che richiedessero tali modalità quale condizione non derogabile per l'erogazione del servizio. Tale eccezione sarà regolata con apposito emendamento al contratto di nomina a RET.

- A seguito di cessazione del rapporto di operatori con il RET, questo è tenuto a comunicarlo al Servizio ICT o SUIC entro 24h allo scopo di procedere all'immediata disabilitazione delle credenziali.

3. Qualsiasi accesso a dati deve essere motivato da esplicita richiesta da parte di AOU o da procedura operativa concordata tra RET e AOU. E' obbligo del RET mantenere documentazione delle motivazioni degli accessi, che AOU si riserva di richiedere in fase di istruttoria relativa a specifici accessi.

4. In nessun caso è consentito il trasferimento di dati in copia unica dalla AOU verso sistemi informativi del RET (es. esportazione di dati storici verso i sistemi del RET con cancellazione dai sistemi di AOU). Anche quando si rendesse necessario trasferire copia di dati verso i sistemi del RET, una copia deve rimanere archiviata sui sistemi di titolarità della AOU o presso l'infrastruttura AOU con modalità concordate con AOU.

5. Eventuali copie di dati verso i sistemi del RET dovranno essere autorizzate (singolarmente o tramite definizione di procedure operative) da AOU e non potranno comunque eccedere l'insieme di dati oggetto del rapporto tra il RET e AOU.

6. Eventuali copie di dati verso i sistemi del RET dovranno essere archiviate e gestite secondo modalità conformi con la normativa vigente e su sistemi che rispettino le Misure Minime di Sicurezza ICT/SUIC definite da AGID come obbligatorie per le pubbliche amministrazioni. La durata dell'archiviazione deve essere limitata al soddisfacimento delle sole esigenze espresse da AOU.

7. Qualsiasi alterazione volontaria di dati (personali o non) da parte del RET sui sistemi di AOU dovrà essere preventivamente esplicitamente autorizzata da AOU.

8. Il RET deve garantire, a conclusione del rapporto, la completa rimozione dei dati di titolarità AOU da ogni supporto o collocazione. Questa dovrà avvenire dopo avere eseguito e documentato con verbale di collaudo il trasferimento dei dati verso destinazione indicata da AOU.

9. E' obbligo del RET notificare alla AOU/Titolare del trattamento entro 12h qualsiasi evento che abbia comportato perdita, alterazione, diffusione o trasmissione non intenzionale verso terzi di dati di AOU. Questo include anche eventi non direttamente imputabili al RET, ma di cui il RET venga a conoscenza.

3. Servizi in Outsourcing Totale

Quanto descritto nella presente sezione si applica al RET il cui rapporto con AOU preveda la fornitura di servizi verso AOU la cui infrastruttura tecnica sia totalmente in gestione al RET (es. soluzioni Cloud quali SAAS, IAAS, PAAS o gestione di sottoreti o sistemi informatici presso i locali di AOU ma a totale carico del RET).

10. Il RET è tenuto a fornire alla AOU una completa descrizione infrastrutturale e architetturale delle modalità di trattamento del dato (informatizzato), che riporti in particolare:

- Collocazione geografica dei data center;
- Modalità di gestione delle credenziali;
- Modalità di gestione degli accessi;
- Modalità di gestione dell'integrità (es. tecnologie di backup);
- Modalità di gestione della confidenzialità (es. architettura di security di rete);
- Modalità di gestione della continuità (es. tecnologie di business continuity).

La AOU si riserva di chiedere approfondimenti tecnici e di rispondenza alle normative della documentazione fornita.

11. Le modalità di trattamento informatico del dato, oltre ad essere conformi alla normativa vigente, devono rispettare le Misure Minime di Sicurezza ICT definite da AGID come obbligatorie per le pubbliche amministrazioni.

12. La AOU si riserva, a titolo di monitoraggio ed ispettivo, di eseguire verifiche remote o sul posto delle modalità di trattamento. Il RET dovrà rendere possibili tali verifiche.

13. Il RET deve fornire una modalità di accesso massivo ai dati di titolarità AOU da parte di un insieme di utenti indicato da AOU. Tale accesso deve consentire in qualsiasi momento una verifica della integrità dei dati, ed essere reso disponibile alla conclusione del rapporto tra RET e AOU per il recupero dei dati e il loro trasferimento su sistemi di gestione

AOU o di altri RET. Tali dati devono essere disponibili in formato leggibile, con strutturazione e codifica documentate e coerenti con le modalità di fruizione e archiviazione applicative (es. non è considerato accesso massivo accettabile il riversamento in formati solo testuali destrutturati, PDF, immagini o comunque non riconducibile a dati strutturati e codificati)

14. Il RET deve garantire l'accesso ai log di sistema (operazioni di accesso e modifica) relativi ai trattamenti dei dati di AOU. Tale accesso deve essere reso disponibile in tempo reale ad un insieme concordato di utenti AOU, o comunque reso disponibile entro 24h dalla richiesta.

15. Il RET deve garantire ad AOU di potere, qualora fossero necessarie operazioni massive sui dati (es. rettifica di dati per prevenire o riparare a malfunzionamenti o errati inserimenti di dati), di poter accedere in modifica con modalità massive ai dati ospitati sui sistemi del RET.

16. Qualsiasi alterazione volontaria di dati (personali o non) da parte del RET sui dati di AOU dovrà essere preventivamente esplicitamente autorizzata dalla AOU.

17. Il RET deve garantire ad AOU di poter oscurare volontariamente e in modo tracciato i dati (pur mantenendo l'oscuramento dell'operazione di oscuramento).

18. Il RET deve garantire, a conclusione del rapporto, la completa rimozione dei dati di titolarità AOU da ogni supporto o collocazione. Questa dovrà avvenire dopo avere eseguito e documentato con verbale di collaudo il trasferimento dei dati verso destinazione indicata da AOU.

19. E' obbligo del RET notificare alla AOU/Titolare del trattamento entro 12h qualsiasi evento che abbia comportato perdita, alterazione, diffusione o trasmissione non intenzionale verso terzi di dati di AOU. Questo include anche eventi non direttamente imputabili al RET, ma di cui il RET venga a conoscenza.

Il Delegato al trattamento
(Dott.ssa Sabrina Amerio)

ACCETTAZIONE DELLA NOMINA

Il legale rappresentante/procuratore di codesta ditta nella sua qualità di Responsabile del trattamento dei dati di cui in premessa:

- accetta la nomina;

- si impegna a procedere al trattamento dei dati personali attenendosi alle disposizioni di cui alla normativa in materia di protezione dei dati personali ed alle istruzioni impartite dal Titolare, Azienda USL di Modena, nel presente Atto o in atti successivi;

- dichiara di aver ricevuto ed esaminato i compiti e le istruzioni sopra indicate
- dichiara di aver preso visione della procedura aziendale per la gestione di Data Breach

per la Ditta/ Responsabile del trattamento

**IL PRESENTE CONTRATTO DEVE ESSERE FIRMATO DIGITALMENTE CON ESTENSIONE PDF
(firma PAdES)**